Multimedia Security

Rich Goyette

29 Nov 04

This presentation was prepared for Professor A. Karmouch in partial fulfillment of the requirements for the course ELG5199 Design of Multimedia Distributed Database Systems

Outline

- Introduction + Motivation
- Content Protection in Transit
  - Encryption
  - *Key Management*
- Content Copyright Protection
  - Watermarking
- *Content Copy Control*
  - *Digital Rights Management (DRM)*

Introduction

- Motivation:
  - Digital representation opens new digital service markets and distribution chains (VoD, superdist, etc);
  - Reproduction is easy and flawless - vast opportunities for wholesale theft;
  - Security is one approach to combat piracy.
- **Encryption** and **watermarking** are complimentary approaches to content protection.
- **DRM** models make use of encryption and watermarking to secure content.

Content Protection

Encryption

Encryption

Definitions ([32][33])

- Digital Content or Content
- Video Compression or *Coding*
  - Uncompressed bit rates for standard (European) television can be as high as 166Mbit/s [32].
  - Compression reduces effective size of sampled video by eliminating spatial and/or temporal redundancy at coder.
  - Greater compression ratios possible if algorithm is "lossy."

Encryption

Definitions ([33])

- Video Transcoding:
  - Aim: to convert coded content from a higher to a lower bit rate (in order to match content coding to channel or device capability);
  - Transcoding can be expensive: pixel domain approach requires full decode, process, and re-code.
  - "Rate Shaping" examples:
    - Spatial down-sampling (resolution change);
    - Frame rate reduction;
    - Change of compression formats or tools;

Encryption

Definitions ([33][34])

- Scalable Compression:
  - Aim: to make transcoding redundant;
  - Encode video once; truncate stream, layers or bits to achieve desired rate or quality.
  - MPEG-2/4 offer "scalability profiles"
    - Eg. MPEG-4 Fine Granular Scalability (FGS):
      - Base Layer encoded to min bit-rate R_b;
      - Progressive enhancement layer encoded to max bit-rate R_m.
      - All devices receive base layer;

Encryption

Definitions ([35][36])

- Motion Picture Experts Group (MPEG) Standards
  - MPEG-1: 1992 – Non-interlaced video up to 1.5 Mbit/s.
  - MPEG-2: 1994 – Interlaced and broadcast video up to 15 Mbit/s.
  - MPEG-4: 1999 – 2GBits/sec and representation of individual objects within frames.
  - Joint Picture Experts Group (JPEG)

Encryption
Approaches

- Secure Scalable Streaming (SSS)
  - Secure Scalable Video Streaming for Wireless Networks (Wee et al. [6])
  - Secure Scalable Video Streaming for Wireless Networks (Wee et al. [7])
- Selective Encryption
  - MPEG video encryption algorithms (Bharagava et al. [3])
- *Adaptive Rich Media Secure*
  - *Securing Media for Adaptive Streaming (Venkatramani et al. [9])*

Encryption

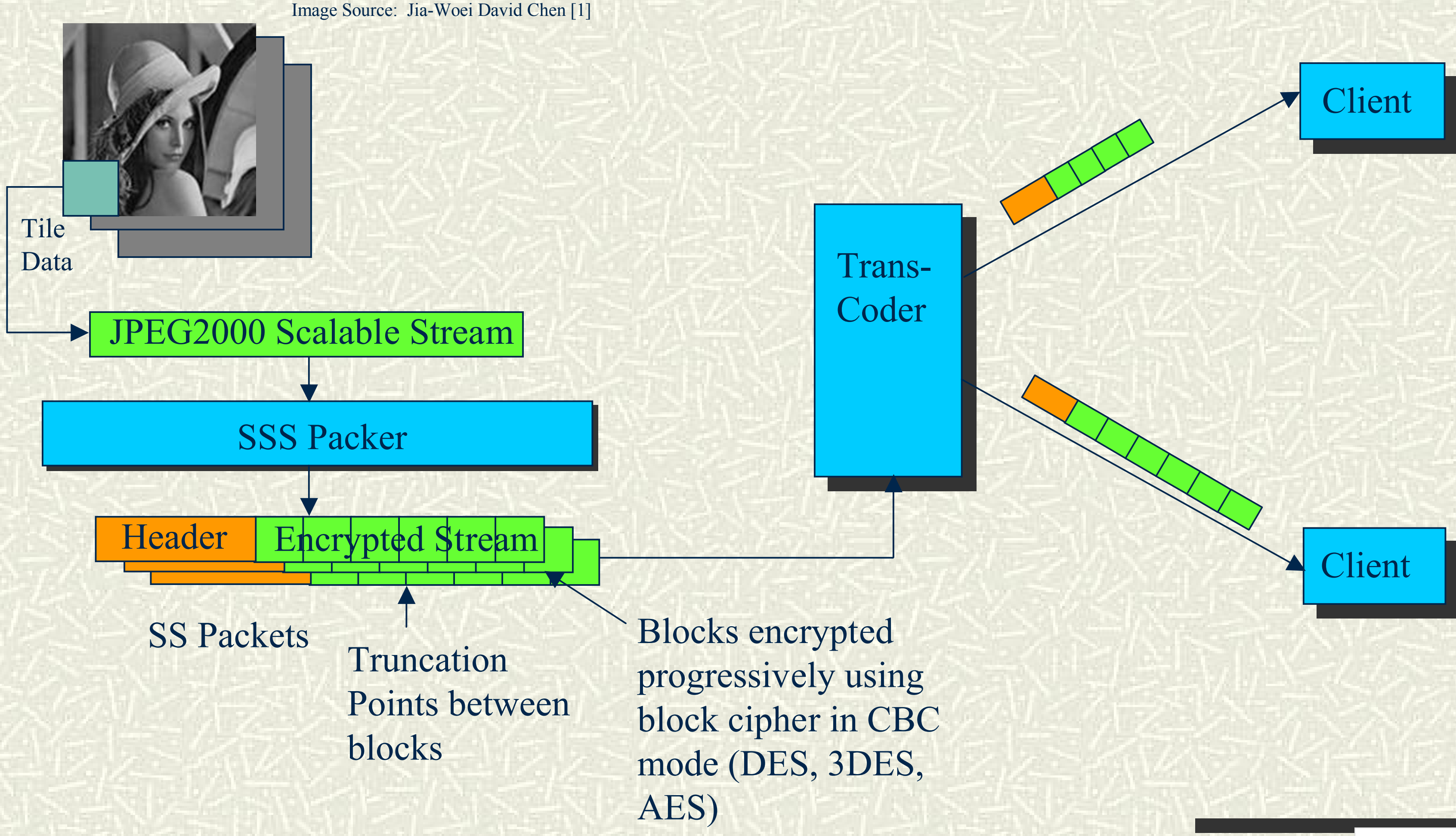
SSS ([6][7])

- "Traditional" transcoding is expensive especially if there are many streams.
- Transcoders need access to secret keys to perform transcoding operations – this introduces a security point-of-failure.
- SSS allows transcoding by intelligent stream truncation:
  - Assumes scalable coding (e.g. JPEG2000, MPEG-4 SNR FGS).

Encryption

SSS ([[6][7])

Image Source: Jia-Woei David Chen [1]



Encryption

Selective Encryption ([3])

- Aim:
  - Render multimedia content incomprehensible without using “heavyweight” encryption.
- Concept:
  - Encrypt small but significant portions of video stream.
  - Employ the (already resource heavy) compression phase to implement the encryption.

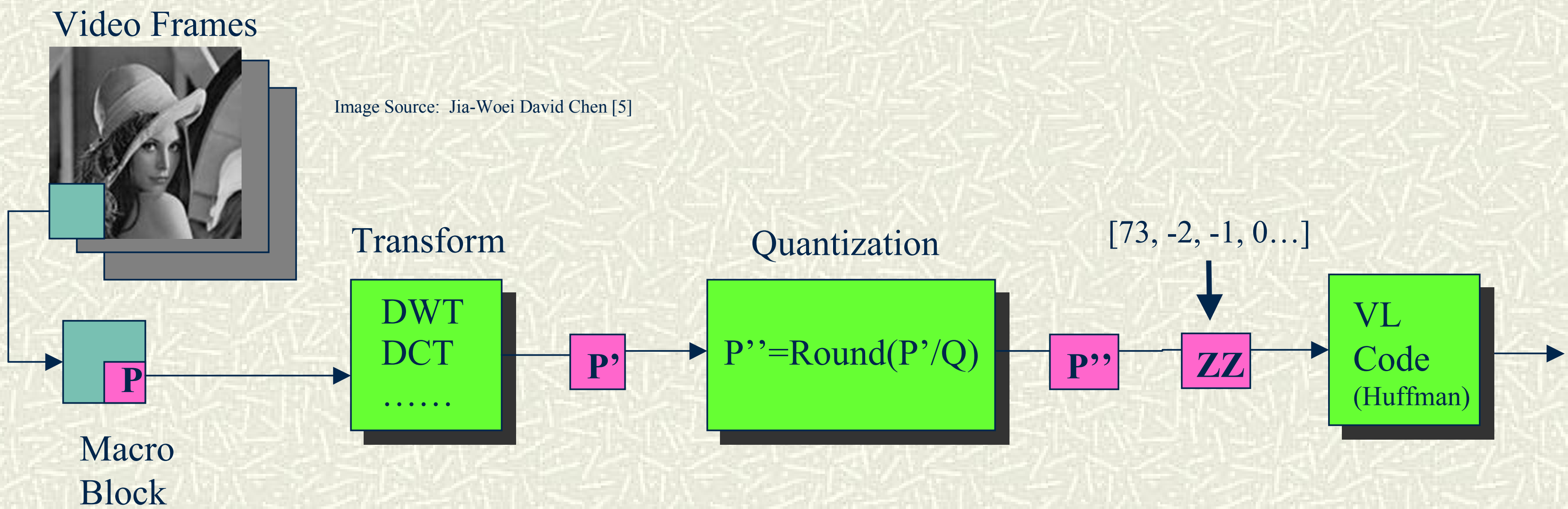
Encryption

Selective Encryption ([3])

- **MPEG Compression mini-tutorial ([3][4][37])**
- Video frames in MPEG are:
  - *Intra*-Frame (spatial) compressed (I-Frame).
  - *Inter*-Frame (temporal) compressed using Motion Compensated Prediction into:
    - P-Frames: Forward predicted MBs
    - B-Frames: Bi-directionally predicted MBs
- A video stream consists of a series of I, P, and/or B frames.

Encryption

Selective Encryption ([3]): *Intra*-Frame Compression



P

67	69	71	72	73	74	75	76
67	69	71	72	73	74	75	76
67	69	71	72	73	74	75	76
67	69	71	72	73	74	75	76
70	70	71	75	78	81	81	75
69	70	71	75	78	80	81	77
68	69	71	74	77	78	80	78
67	69	71	74	76	76	78	80

P'

587	-27	-5	1	-1	1	-1	0
-8	5	1	-3	0	-1	1	0
-2	-1	1	-3	1	-1	0	0
5	-1	-2	4	-1	1	-1	0
-1	0	0	0	0	0	0	0
-3	0	1	-2	0	0	0	0
0	0	0	0	0	0	0	0
2	0	-1	2	-1	1	0	0

Q (MPEG-1)

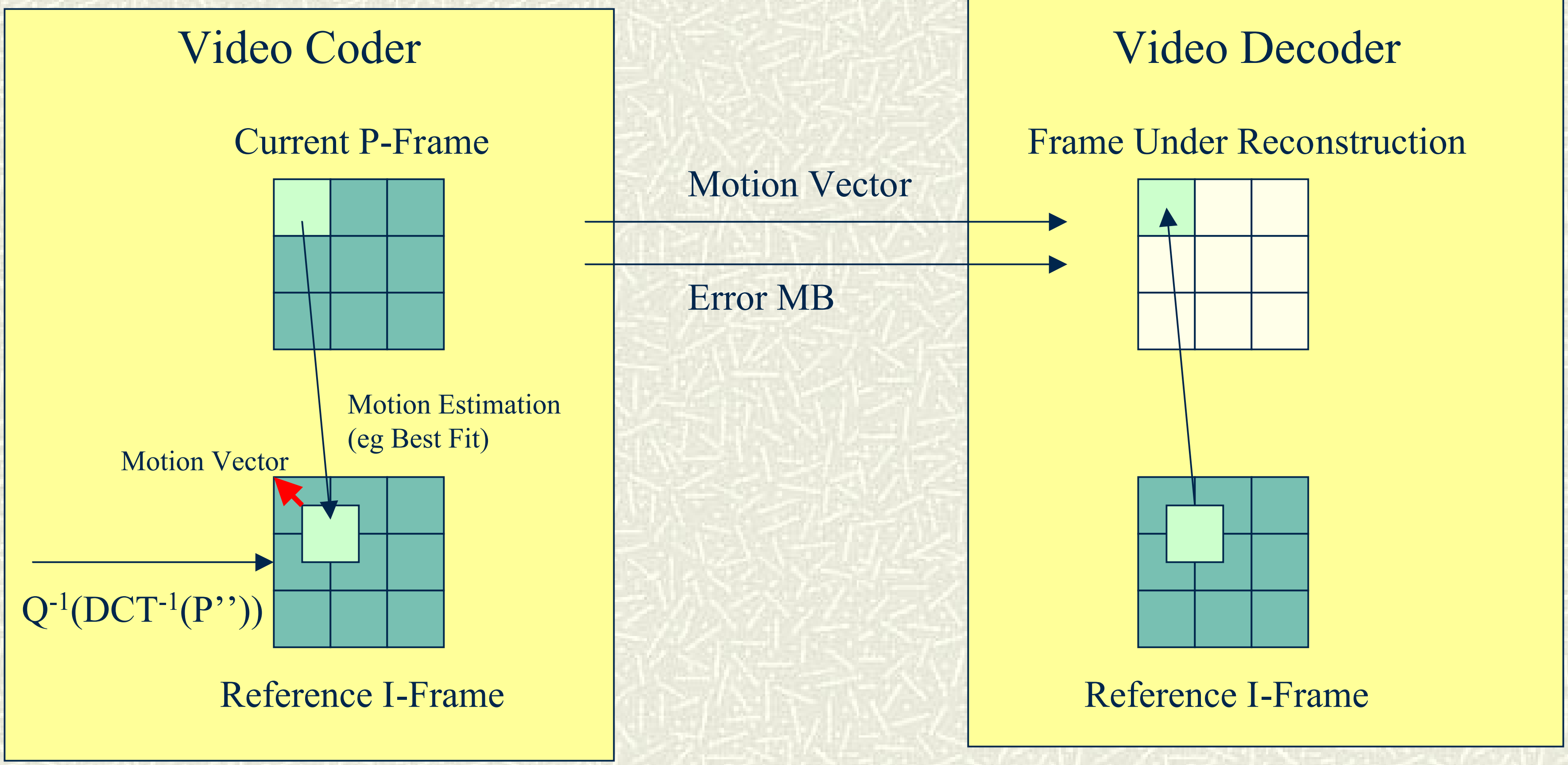
8	16	19	22	26	27	29	34
16	16	22	24	27	29	34	37
19	22	26	27	29	34	34	38
22	22	26	27	29	34	37	40
22	26	27	29	32	35	40	48
26	27	29	32	35	40	48	58
26	27	29	34	38	46	56	69
27	29	35	38	46	56	69	83

P''

73	-2	0	0	0	0	0	0
-1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Encryption

Selective Encryption ([3]): *Inter*-Frame Compression



References: Figure 2 of [3] and slides 46-56 of [4]

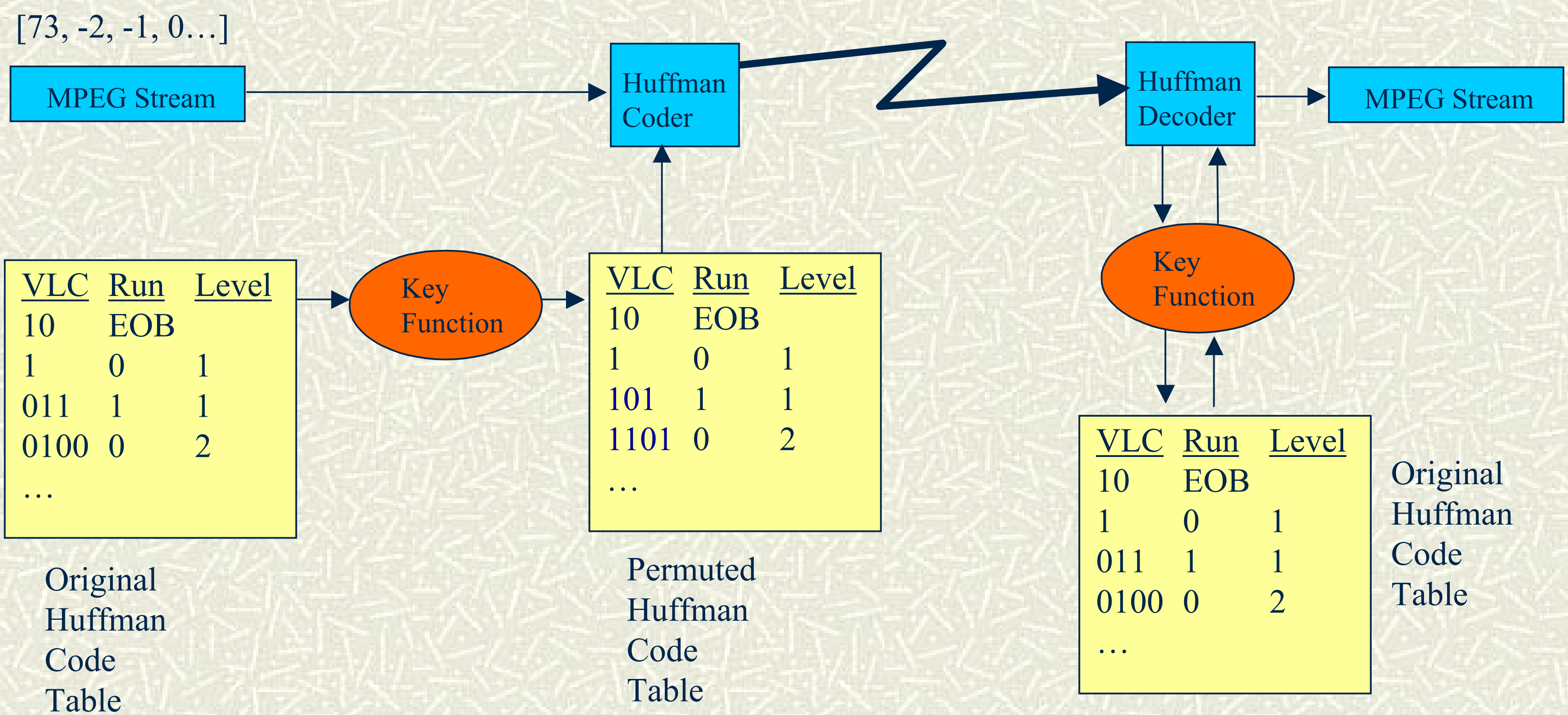
Encryption

Selective Encryption ([3])

- Review of selective encryption (Liu et al. [8]) includes the following approaches for Video stream encryption in frequency domain:
  - Encrypt I-frames, DCT coefficients, sign bits of motion vectors, every other bit of MPEG stream, every nth I-frame macroblock, etc.
  - Randomizing "zig-zag" pattern prior to VLC.
- Algorithms proposed in Bhargava et al.:
  - Huffman Permutation, VEA, MVEA, and RVEA

Encryption

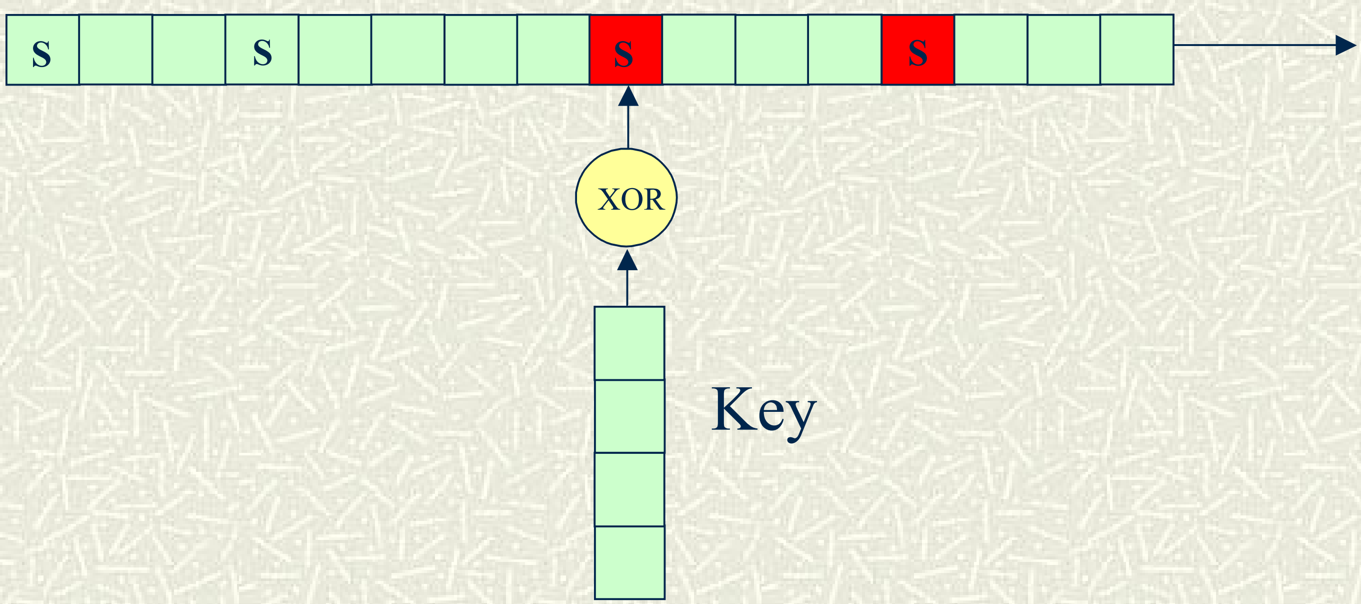
Selective Encryption: a.) Huffman Permutation [3]



Encryption

Selective Encryption: b.) Video Encryption Algorithm (VEA) [3]

- An m-bit key is randomly produced and XORed with the sign bits of DCT components in I-Frames.



Encryption

Selective Encryption: b.) Video Encryption Algorithm (VEA) [3]

- Results in apparent "randomization" of sign bits.
- Increasing length of secret key does not increase complexity.
- Security relies on inverse-DCT process to "scramble" the video image.
- Weak against plaintext attacks.

Encryption

Selective Encryption: c.) Modified VEA (MVEA) [3]

- An m-bit key is produced as in VEA.
- Sign bits of DC components in I-Frames are encrypted.
- Sign bits of motion vectors in B and P Frames are encrypted – this has significant effect on reconstruction since changing motion vector sign changes direction.
- Also weak to plaintext attacks.

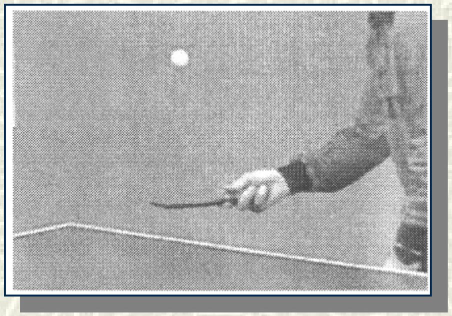
Encryption

Selective Encryption: d.) Robust VEA (RVEA) [3]

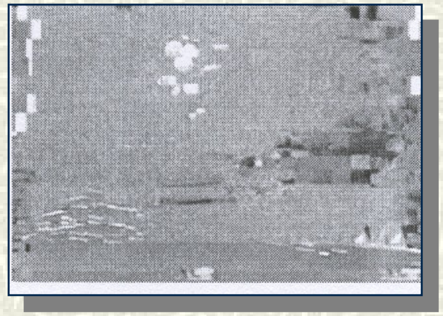
- Same as MVEA except that m-bit key and XOR is replaced by “heavyweight” symmetric encryption of sign bits.
- Since sign bits make up less than 10% of stream data, this use of “heavyweight” encryption is still more efficient than encrypting whole payload.

Encryption

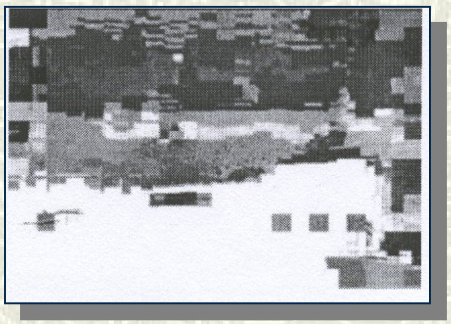
Selective Encryption: Sample Experimental Results from [3]



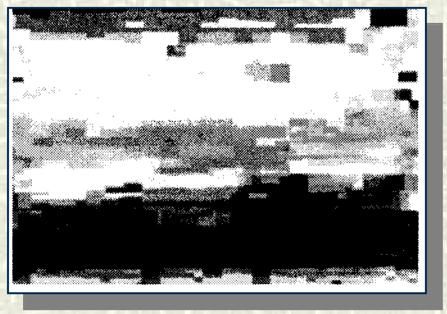
Original Video Frame
(Figure 9 of [3])



MVEA on B frame
Motion vectors only
(Figure 13 of [3])



VEA on I-Frames
(Figure 12 of [3])



RVEA
(Figure 14 of [3])

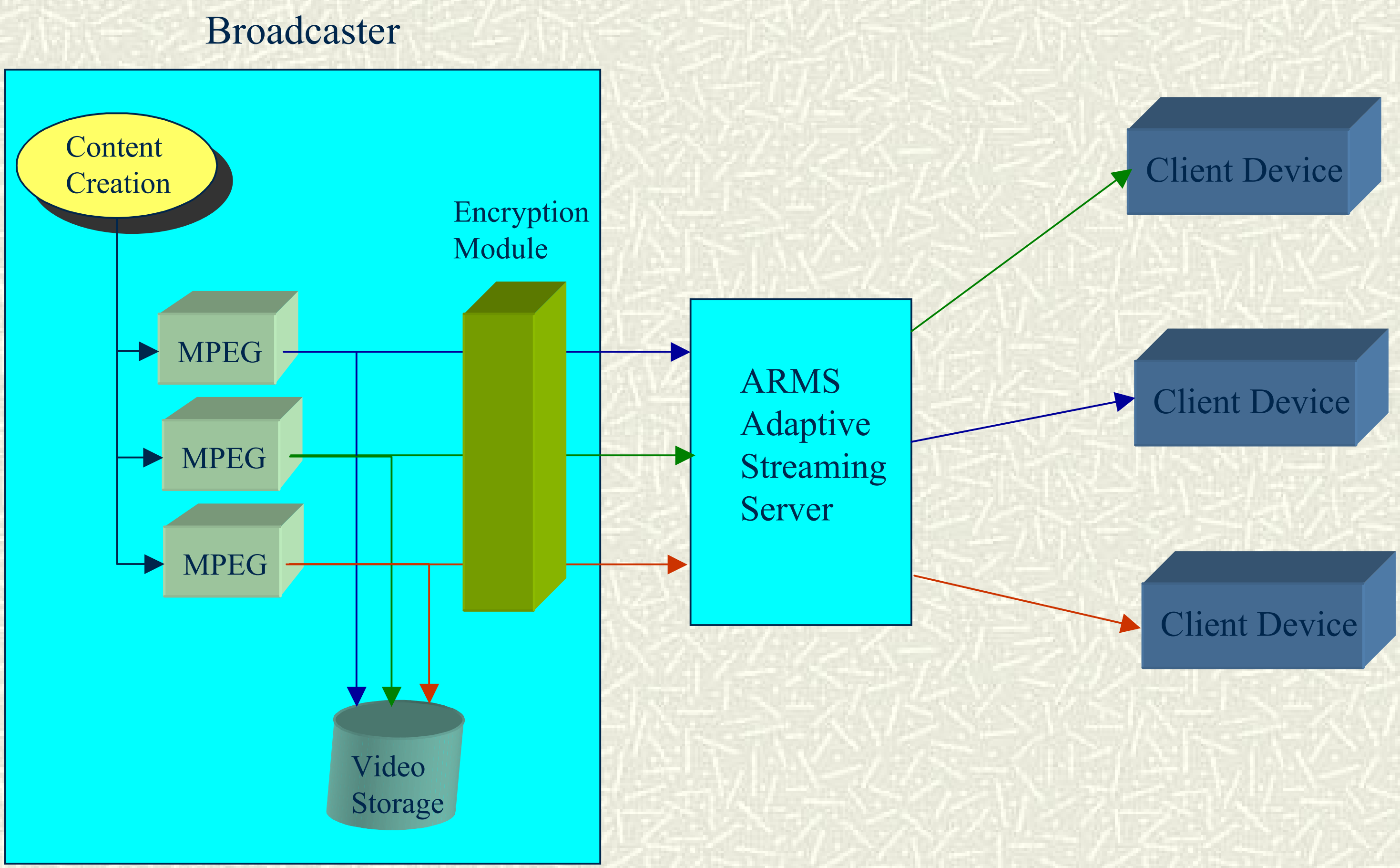
Encryption

Adaptive Rich Media Secure – ARMS ([9])

- Uses Internet Streaming Media Alliance (ISMA) standard for *secure content delivery (RTP over UDP)*.
- Uses stream cipher with encryption index to allow resync in event of packet loss (compare with SSS).
- Modifies ISMA to allow for multiple streams and stream switching.
- ARMS is basis of IBM VideoCharger system.

Encryption

Adaptive Rich Media Secure – ARMS ([9])



Ref: Figure 4 from [8]

Encryption

Summary of Video Encryption Approaches

	SSS	Selective Encryption	ARMS
Overhead	*Packet* overhead of 2-2.5% compared to end-to-end encryption.	No packet overhead. Software VEA *processing* time overhead of 1.8%. RVEA consumes 2.5% of time during compression.	ISMA meta data (unknown size) compared to end-to-end encryption..
Specialized streaming hardware required	Yes - SSS transcoder.	No	Streaming Server
Client modifications required	Yes - SSS aware client.	Yes.	Yes - ISMA aware client.

Copyright Protection

Digital Watermarking

Watermarking

- Digital Watermarking: Information is inserted directly into a multimedia object at the expense of a (hopefully) imperceptible degradation in the quality of that object.
- Has parallels with paper watermarking and steganography or data hiding.
- Complimentary to encryption and being invested in as a DRM solution.

Watermarking

Uses [11][16][17]

- Uses of Watermark schemes:
  - Identification of content origin (proof of ownership or authorship watermarks);
  - Tracing of illegally distributed copies of content (fingerprinting watermarks); and
  - *Disabling unauthorized access to content*.

Watermarking

Properties [11][18][19][20]

- Properties of Watermarks:
  - Robustness against both un-intentional attacks (standard data processing – compression, zooming, cropping, etc) and intentional attacks
  - Fragile
  - Imperceptible
  - Visible
  - Unambiguous

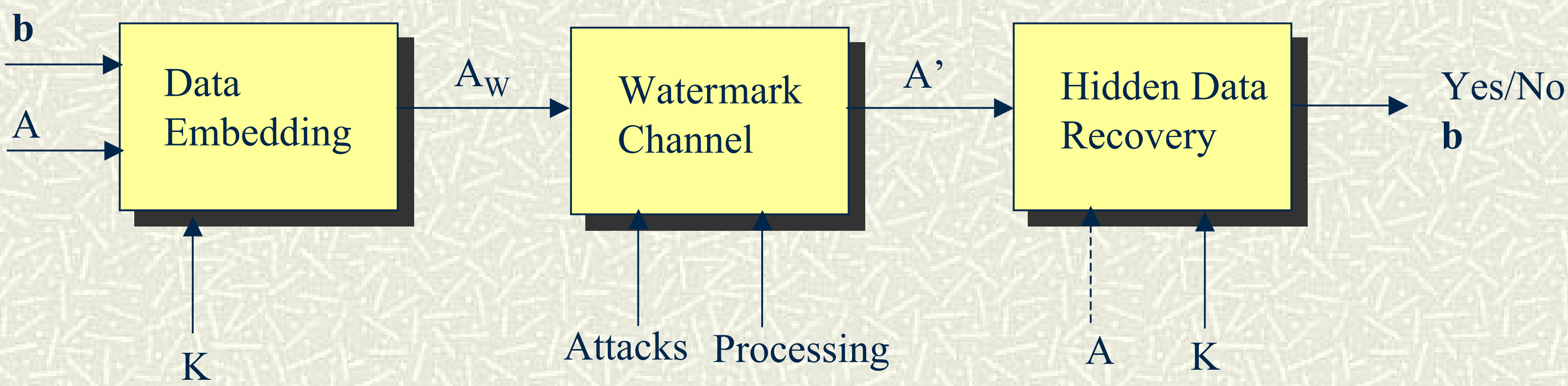
Watermarking

Blind vs Informed [19][21]

- Watermarking process can be:
  - Blind:
    - Watermark has no dependency on the "cover" object.
    - Original, unmarked object not needed to extract or detect watermark.
    - Typically blind watermarks use spread spectrum techniques where cover is considered to be "noise."
  - Informed:
    - Watermark signal depends on cover object.
    - For example, delta is added to higher frequency DCT coefficients to map them to detector decision regions.

Watermarking

System Model [16]



b=(b1, b2, b3, …)	The watermark information in the form of a binary string.
A	The original, unmarked media to be watermarked (also known as the cover media).
K	A cryptographic key which may be either symmetric or asymmetric.
Aw	A watermarked media.
A’	A watermarked media that has passed through the watermark channel.

Ref: Figure 1 of [16]

Watermarking

Watermark Attacks ([18][22][23])

- Watermark “attacks” drive research.
- Example attacks:
  - Protocol Attacks against Authorship Watermarks
  - *Attacks against FingerPrint Watermarks*
    - *Collusion Attacks*
    - *Protocol Attacks*

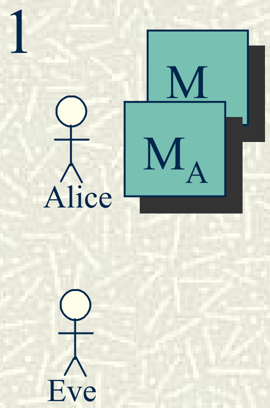
Watermarking

Protocol Attacks Against Ownership Watermarks ([23][24])

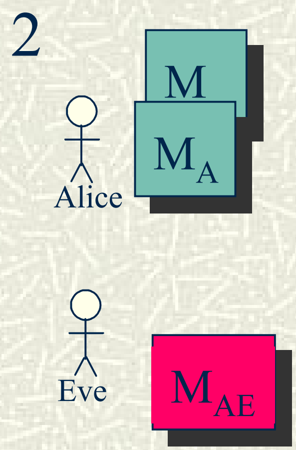
- Protocol attacks target the dispute resolution process rather than trying to remove the watermark.
- Protocol attacks introduce ambiguity and uncertainty in ownership.
- Types [24]:
  - Copy Attack – copy existing watermark from object A to B.
  - Ambiguity Attack – compute a watermark that was never inserted but can still be found in an object.

Watermarking

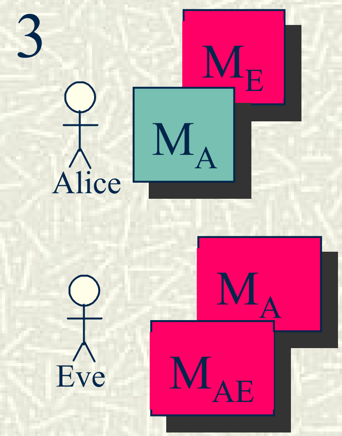
Single Watermarked Image Counterfeit Original (SWICO) ([23])



Alice creates watermarked object M_A from original M.



Eve examines M_A and finds a set of arbitrary features to call her watermark (E). She designs a detector to find this watermark.. This results in M_{AE}. Note that Alice's M also contains E.



Eve removes arbitrary features from MA to get her "original" M. Eve's M contains A and Alice's M contains E. So who owns M?

Watermarking

Protocol Attack Defences

- Approaches to eliminate protocol attacks:
  - Restrict degrees of freedom in selecting or designing watermark components [25]
  - Eliminate or limiting some attacks through cryptographic signatures and third party validation of watermarks [24].
  - Trusted time stamps.

Conclusions

- Encryption and Watermarking are at the forefront of research into content protection.
- Personal Learning Goals:
  - Technical details of MPEG.
  - Scoping a wide arc of research.
  - Research resources/techniques.

Questions?

Supplementary Material

- Key Management in Conditional access sytems;
- Digital Rights Management;

Content Protection

Key Management

Key Management

- Encryption techniques usually "assume" key management infrastructure.
- Key management for conditional access (CA) systems.
- CA systems are most prevalent form of broadcast encryption [10] and include:
  - Video on Demand
  - Subscription channels and Pay-Per-View [12]

Key Management

Characteristics ([2][11][13])

- Key management must:
  - Deal efficiently with end-user turnover:
    - Joins must not be able to access material already *casted; and
    - Leaves must not be able to access material that will be *casted
  - Have minimal impact on end-user processing;
  - Be scalable; and
  - Be resilient to key compromise (us).

Key Management

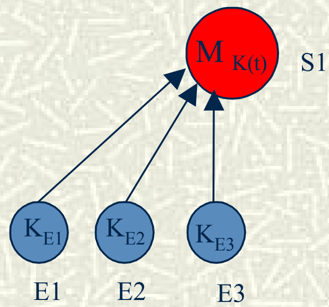
Approaches

- Flat or Star topology
  - Secure Group Communications using Key Graphs (Wong et al. [1]).
  - Key Management and Distribution for Secure Multimedia Multicast (Trappe et al. [2])
- Key Graph Model
  - Secure Group Communications using Key Graphs (Wong et al. [1]).
- Secret Sharing with Key Graphs
  - Multicast Security using Key Graphs and Secret Sharing (Eskicioglu et al. [13])
  - A Key Transport Protocol Based on Secret Sharing Applications to Information Security (Eskicioglu et al. [14])

Key Management

Flat or Star (Reference) Topology ([1][2])

- Flat or "Star" topology is most intuitive;



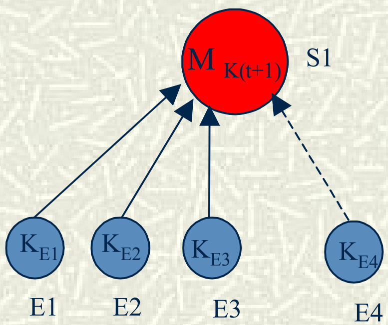
Ref: Figure 1 of [1]

- Characterized by server S1, end-users E_n.
- Multimedia data encrypted with Media key $M_{K(t)}$.
- End users have $M_{K(t)}$ and K_{En} used for key update operations.

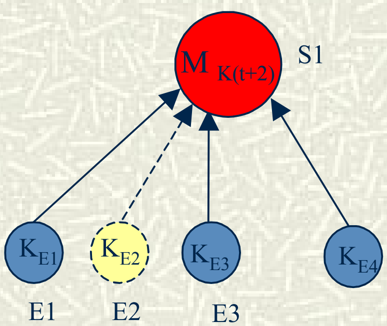
Key Management

Flat or Star (Reference) Topology ([1][2])

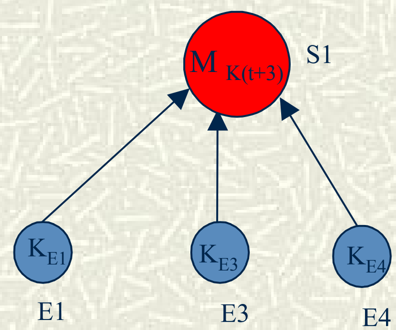
User Joins, Leaves and Key Update operations for Star Topology



CASE 1
E4 Joins:
1. $\{M_{K(t+1)}\}M_{K(t)}$
2. S1<->E4: K_{E4}
3. $\{M_{K(t+1)}\}K_{E4}$



CASE 2
E2 Leaves:
1. $\{M_{K(t+2)}\}K_{E1}, K_{E3}, K_{E4}$



CASE 3
Key Update:
1. $\{M_{K(t+3)}\}K_{E1}, K_{E3}, K_{E4}$

Refs: Figures 2 and 3 of [1]

Key Management

Flat or Star (Reference) Topology ([1][2])

- Obvious limitations of flat topology:
  - Leave operations and key updates require:
    - (n-1) encryptions by server;
    - (n-1) unicasts.
  - Star topology is un-scalable: complexity of server computation, communication, and storage requirements is linear.

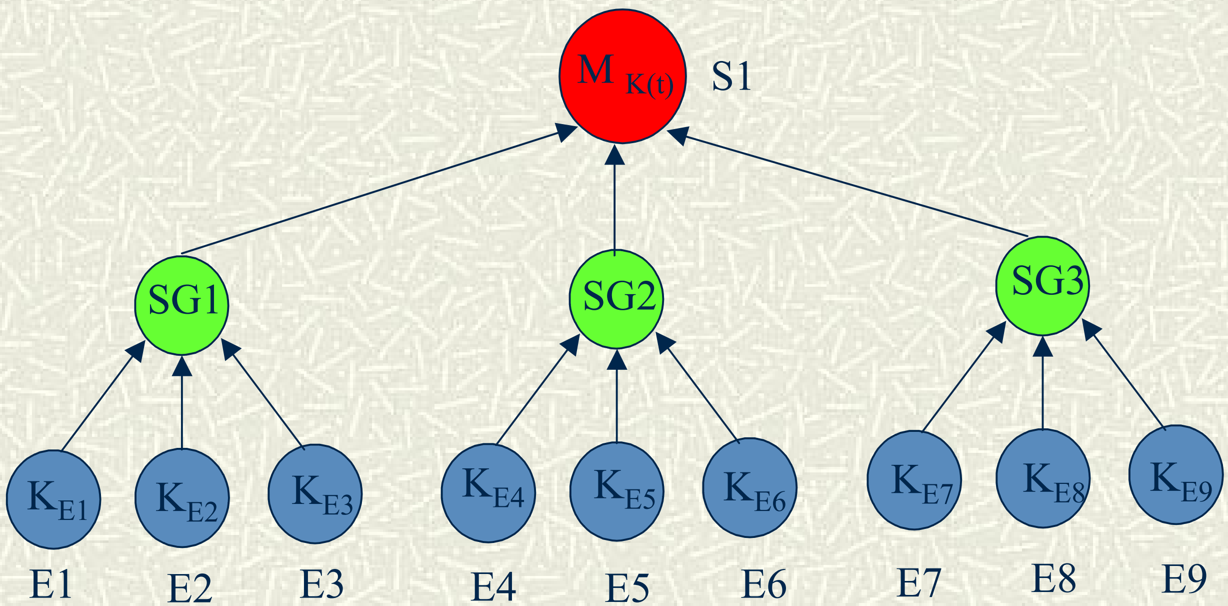
Key Management

Key Graph Model ([1])

- Wong's key graph model seeks to address scalability of star topology by introducing "subgroups"
- Server creates a key graph with n-leaves and a symmetric key at each node.
- K-nodes have keys only. M-nodes are end-users who retain a subset Q of Server's keys.
- Subset Q includes all keys in directed path to root node.

Key Management

Key Graph Model ([1])

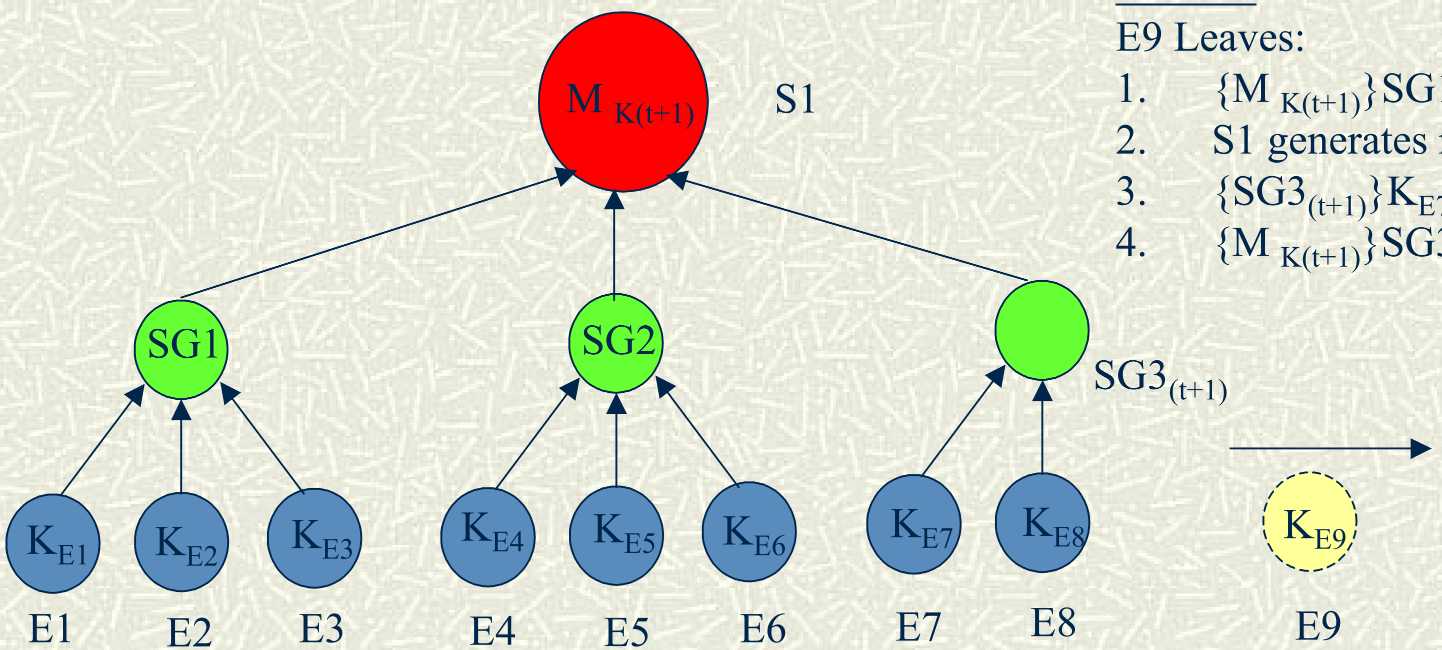


Each user E_n has $\{ M_{K(t)}\ SG_n\ K_{en} \}$

Ref: Figure 5 of [1]

Key Management

Key Graph Model ([1])



CASE 2

E9 Leaves:

1. $\{M_{K(t+1)}\}$SG1, SG2
2. S1 generates new key $SG3_{(t+1)}$
3. $\{SG3_{(t+1)}\}K_{E7}, K_{E8}$
4. $\{M_{K(t+1)}\}SG3_{(t+1)}$

Each user E_n has $\{ M_{K(t+1)}\ SG_n\ K_{en} \}$

Ref: Figure 5 of [1]

Key Management

Key Graph Model ([1])

- A user "leave" operation in the example involves five encryptions instead of eight.
- Key-update in the example involves three encryptions instead of nine.
- In a balanced tree with many users, the savings can be substantial.

Key Management

Secret Sharing With Key Graphs ([13][14])

- "Secret Sharing" for key distribution:
  - Uses threshold scheme where secret **S** is composed of **n** shares. User needs **t** of **n** shares to determine **S**.
  - Threshold scheme used by authors is based on A. Shamir's (t,n) thresholding scheme ([15]).

Key Management

Secret Sharing With Key Graphs ([13][14])

- Secret sharing example:
  - Pre-position (t-1) points [(x_1,y_1), (x_2,y_2)…] with end-user;
  - Choose secret S as point on Y axis (0,S);
  - Determine (t-1) degree polynomial f(x) that fits points [(x_1,y_1), (x_2,y_2)…] and (0,S).
  - Choose "activating share" point (x_n, y_n) s.t. $y_n=f(x_n)$ and (x_n, y_n) is not equal to any of [(x_1,y_1), (x_2,y_2)…] .
- To pass the secret, pass (x_n,y_n) to end-user (who now has t points on a (t-1) degree polynomial).
- Solve system of equations to determine a_0=(0,S).
- Secret can be changed without changing the pre-positioned information.

Key Management

Secret Sharing With Key Graphs ([13][14])

- CKMSS combines key graph model with secret sharing.
- In the key graph, wherever a key is found, a set of shares is distributed instead.
- Media, group, and client keys are generated at the end-user by sending an activating share (in the clear).

Key Management

Secret Sharing With Key Graphs ([13][14])

- Chief advantages of Secret Sharing with Key Graphs:
  - Periodic re-keys require multicast of fixed length "activating share" that does not need to be encrypted.
  - Simulation shows that increasing number of shares per node (degree of the polynomial) is "mildly non-linear."

Content Copy Control

Digital Rights Management (DRM)

DRM

- DRM: “a collection of technologies that enable technically enforced licensing of digital information” [26]
- DRM promises finer-grained control of content usage but:
  - Challenges currently accepted models of “fair use”; and
  - Invokes privacy concerns.

DRM

- Elements of a DRM system;
- Approaches to DRM:
    - Top down (MPEG-21)
    - Bottom up (OMA MDRM)
    - Legal approaches

DRM

Elements of DRM ([27])

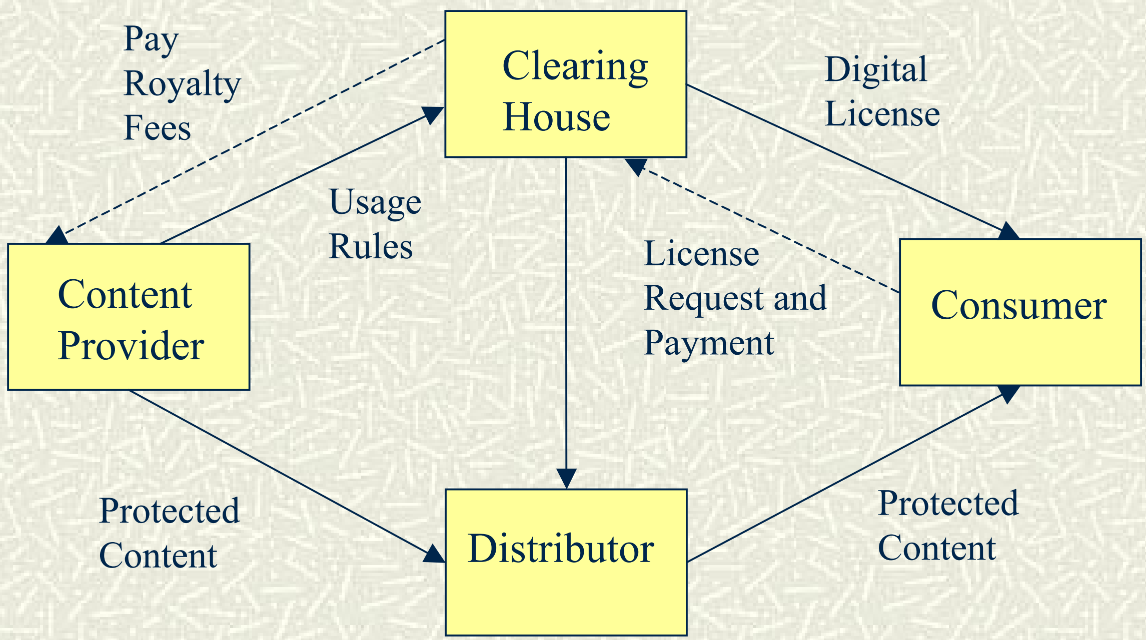


Figure 2.1 of [27]

DRM

Model Requirements

- Examination of the model reveals:
  - Need for a comprehensive REL;
  - Critical requirement for "trusted" clients to enforce licenses against content;
  - Privacy is an issue – licenses are issued to "entities."
  - Standardization is essential to avoid "stove-pipes."

DRM

Trusted Computing ([28])

- Trusted Computing is the “lynch-pin” of all DRM systems. The client must ensure that:
  - The client cannot remove the encryption from the file and send it to a peer;
  - The client obeys the rules set out in the DRM license; and
  - The client cannot separate the rules from the payload

DRM
Trusted Computing

- No sufficient general purpose trusted computing platform exists (yet).
- Work is under way:
  - Trusted Computing Group (not targeted towards DRM [29]);
  - Microsoft Next Generation Secure Computing Base (NGSCB) (formerly Palladium).([30][31])

DRM

Top Down Approach: MPEG-21

- Top-down approach: MPEG-21
- MPEG-21 seeks to
  - understand, integrate, and standardize all of the disparate elements that exist *now* for DRM
  - to perform a gap analysis; and
  - to fill in where standards appear to be lacking
- MPEG-21 is attempting to build the "big picture" of digital rights management

DRM

Top Down Approach: MPEG-21

- MPEG-21 Parts:
  - Vision, technologies, and strategies (introduction);
  - Digital Item Declaration (DID);
  - Digital Item Identification (DII);
  - Intellectual Property Management and Protection (IPMP) (continues MPEG-4 hooks to proprietary systems)
  - Rights Expression Language (REL);
  - Rights Data Dictionary (RDD); and
  - Digital Item Adaptation (DIA);

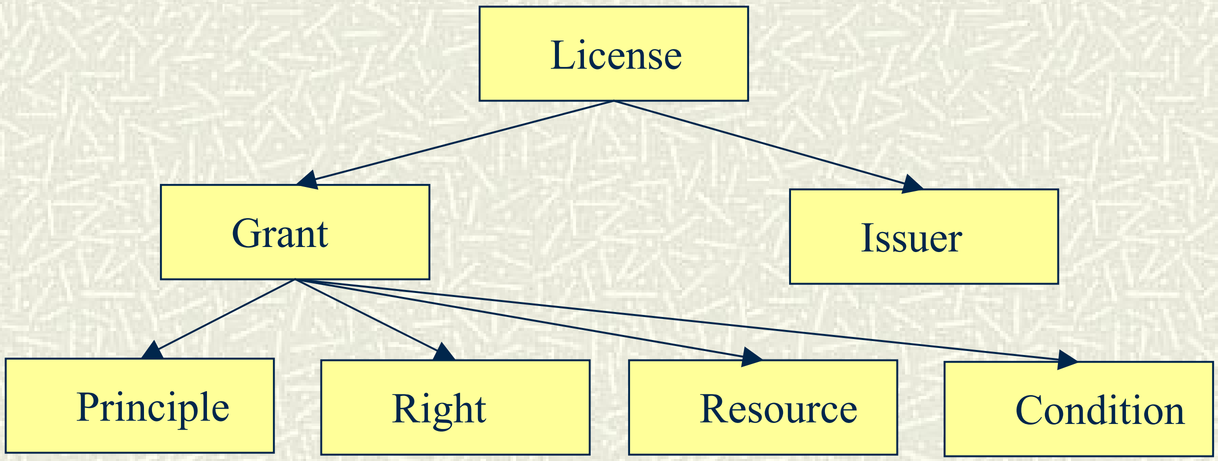
DRM

Top Down Approach: MPEG-21

- MPEG-21 REL
  - Based on ContentGuard’s XrML
  - Achieved standard status in early 2004.
  - *License* is most important concept in REL.

DRM

Top Down Approach: MPEG-21



MPEG-21 "License"

Ref: figure 3 wang

DRM

Bottom-Up Approach: OMA MDRM

- Bottom-up approach: OMA Mobile DRM
  - Open Mobile Alliance founded 2002.
  - Goal: introduce open DRM standards for mobile devices.
  - OMA scoped initial effort to devices with limited processing and memory (cell phones).
  - This approach lead to fast development of OMA MDRM 1.0 and *rapid* market adoption across resource limited devices.

DRM

Bottom-Up Approach: OMA MDRM

- OMA standard for REL is based on Open Digital Rights Language (ODRL).
- OMA MDRM 2.0 released in 2004:
  - Targets devices with more processing/memory;
  - Adds new security features (public key enc);
  - Expands business models.
- At some point, MDRM will meet MPEG-21.

DRM

Bottom-Up Approach: OMA MDRM

- Legal Approaches: DMCA
- DMCA is U.S. copyright law passed in 1998.
- Specifically bans:
  - Acts that circumvent access control/copy prevention mechanisms; and
  - Distribution of tools/technologies/information that allow circumvention.

DRM

Bottom-Up Approach: OMA MDRM

- Unintentional side effects of DMCA:
  - Stifles academic research (Felton vs Secure Digital Music Initiative);
  - Allows censorship of 2600 Magazine's web site and publication (DeCss) contrary to U.S. 1st Amendment Free Press.
  - Used by Lexmark as a business weapon against after-market toner makers.

References (1/4)

[1] C. Wong, M. Gouda, and S. Lam, "Secure group communications using key graphs," *IEEE/ACM Transactions on Networking*, vol. 8, no. 1, pp. 16-30, February 2000.

[2] W. Trappe, J. Song, R. Poovendran, and K. Ray Liu, "Key management and distribution for secure multimedia multicast," IEEEE Transactions on Multimedia, vol. 5, no. 4, December 2003.

[3] B. Bharagava, C. Shi, and S. Wang, "MPEG video encryption algorithms," *Multimedia Tools and Applications*, vol 24, pp. 57-79, Sept 2004.

[4] Geckle, W. "MPEG Video Compression, Lecture 10," available at www.apl.jhu.edu/Notes/Geckle/525759

[5] Jia-Woei David Chen www.personal.psu.edu/users/j/u/juc169/fall2004_ee485chen_proj0.htm

[6] S. Wee, and J. Apostolopoulos, "Secure scalable video streaming for wireless networks," *IEEE International Conference on Acoustics, Speech, and Signal Processing*, Salt Lake city, Utah, May 2001.

[7] S. Wee, and J. Apostolopoulos, "Secure scalable video streaming for wireless networks," *Proceedings, International Conference on Image Processing,* vol. 1, pp. 205-208, 2003.

[8] X. Liu, A. Eskicioglu, "Selective encryption of multimedia content in distribution networks: challenges and new directions," *IASTED International Conference on Communications, Internet and Information Technology (CIIT 2003)*, Scottsdale, AZ, November 17-19, 2003.

[9] C. Venkatramani, P. Westernink, O. Versheure, and P. Frossard, "Securing media for adaptive streaming," *Proceedings of the Eleventh International Conference on Multimedia*, pp. 307-310, 2003.

[10] W. Jonker and JP Linnartz, "Digital rights management in consumer electronics products," IEEE Signal Processing Magazine, March 2004, pp. 82-91.

[11] A. Eskicioglu, "Multimedia security in group communications: recent progress in key management, authentication, and watermarking," Multimedia Systems, vol. 9, pp. 239-248, 2003. (www.sci.brooklyn.cuny.edu/~eskicioglu/papers/index.html)

[12] YL Huang, S. Shieh, FS Ho, and JC Wang, "Efficient key distribution schemes for secure media delivery in Pay-TV systems," IEEE Transactions on Multimedia, vol. 6, no. 5, October 2004.

References (2/4)

[13] A. Eskicioglu and M. Eskicioglu, "Multicast security using key graphs and secret sharing," Proceedings of the Joint International Conference on Wireless LANs and Home Networks (ICWLHN 2002) and Networking (ICN 2002), pp. 228-241, Atlanta, GA, August 26-29, 2002. (www.sci.brooklyn.cuny.edu/~eskicioglu/papers/index.html)

[14] A. Eskicioglu and E. Delp, "A key transport protocol based on secret sharing applications to information security," *IEEE Transactions on Consumer Electronics*, vol. 48, no. 4, pp. 816-824, November 2002. (www.sci.brooklyn.cuny.edu/~eskicioglu/papers/index.html)

[15] A. Shamir, "How to share a secret," Communications of the ACM, vol.22, no. 11, pp. 612-613, November 1979. Available at http://crypto.csail.mit.edu/classes/6.857/papers/secret-shamir.pdf.

[16] M. Barni and F. Bartolini, "Data hiding for fighting piracy," IEEE Signal Processing Magazine, March 2004, pp. 28-39.

[17] D. Kundur and K. Karthik, "Video fingerprinting and encryption principles for digital rights management," Proceedings of the IEEE, vol. 92, no. 6, June 2004.

[18] A. Kejariwal, "Watermarking," IEEE Potentials Magazine, October/November 2003, pp. 37-40.

[19] F. Petitcolas, R.J. Anderson, and M. Kuhn, "Information hiding – a survey," Proceedings of the IEEE, pp. 1062-1078, July 1999.

[20] F. Hartung and M. Kutter, "Multimedia watermarking techniques," Proceedings of the IEEE, vol. 87, no. 7, July 1999.

[21]* M. Barni ed. Signal Processing Magazine Forum Article "What is the future for watermarking? (part II)," IEEE Signal Processing Magazine, November 2003.

[22] F. Petitcolas, and R.J. Anderson, "Evaluation of copyright marking systems," Proceedings of IEEE Multimedia Systems'99, vol. 1, pp. 574-579, 7-11 June 1999, Florence, Italy.

[23] S. Craver, N. Memon, B.L. Yeo, and M. Yeung, "Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, and implications," IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, May 1998.

References (3/4)

[24] A. Adelsbach, S. Katzenbeisser, and H. Veith, "Watermarking schemes provably secure against copy and ambiguity attacks," Proceedings of the 2003 ACM Workshop on Digital Rights Management, 27 October 2003, pp. 111-119.

[25] M. Ramkumar and A. Akansu, "A robust protocol for proving ownership of multimedia content," IEEE Transactions on Multimedia, vol. 6, no. 3, June 2004.

[26] R. Koenen, J. Lacy, M. Mackay, and S. Mitchel, "The long march to interoperable digital rights management," Proceedings of the IEEE, vol., 92, no. 6, June 2004.

[27] Q. Liu, R. Safavi-Naini, and N. Sheppard, "Digital rights management for content distribution," Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003, vol. 21, pp 49-58.

[28]* P. Biddle, P. England, M. Peinado, and B. William, "The darknet and the future of content distribution," in *Digital Rights Management: Technological, Economic, Legal and Political Aspects*, ed E. Becker, W. Buhse, D. Gunnewig, N. Rump (Springer-Verlag, 2003).

[29] R. Enderle, "Trusted computing: maligned by misrepresentations and creative fabrications," Storage Pipeline e-magazine, 02 May 2004 (attached).

[30] T. O'Reilly, "Microsoft patents 'Digital Rights Management Operating System'", 13 Dec, 2001, available at www.oreillynet.com/cs/user/view/wlg/956 (attached).

[31] K. Coyle, Digital Rights Management – Part 4. Available at www.kcoyle.net/drm_basics4.html (attached).

[32] P. Tudor, "MPEG-2 video compression," *IEE Electronics and Communication Engineering Journal*, December 1995.

[33] A. Vetro, C. Chritopoulos, H. Sun, "Video transcoding architectures and techniques: an overview," *IEEE Signal Processing Magazine*, pp. 18-29, March 2003.

[34] H. Radha, M. van der Schaar, and Y. Chen, "The MPEG-4 fine-grained scalable video coding method for multimedia streaming over IP," *IEEE Transaction on Multimedia*, vol. 3, no. 1, March 2001.

References (4/4)

[35] Video Compression Tutorial, Wave Report, located at www.wave-report.com/tutorials/VC.htm.

[36] R. Koenen, "Object-based MPEG offers flexibility," *EE Times*, 12 November, 2001, located at www.eetimes.com.

[37] Geckle, W. “MPEG Video Compression, Lecture 9,” available at www.apl.jhu.edu/classes/Geckle/525759