Video Casting Application Oriented Key Exchange

Abdullah Rashed and Henrique Santos
Algortimi Centre
University of Minho
Guimaraes, Portugal
rashed@dsi.uminho.pt / hsantos@dsi.uminho.pt

***Abstract*— Within video stateless receivers, a central server should deliver information securely to the authorized users, over a public channel, even if receivers do not update their state from session to session. This is the case of a multimedia conditional access systems based on one way broadcasting. This paper suggests a new approach to assure a secure communication in such environments. The proposed approach is an efficient key exchange scheme for stateless receivers. It reduces the number of private keys used in traditional conditional access systems and the number of encryptions operations as it does not need to encrypt the ciphering keys. Furthermore, the presented approach eliminates the required key refreshment presented in other approaches. We tested the proposed system using AES algorithm. A numerical example is used to demonstrate the effectiveness of the presented approach. This technique can be very useful for small devices, with limited resources and strict power consumption requirements, which are becoming prevalent in multimedia Conditional Access Systems (CAS) one way broadcasting.**

Keywords-Key exchange; Broadcast Encryption; Conditional Access Systems.

I. INTRODUCTION

Security of digital multimedia transmission is very important due to the communication explosion [1]. It is widely used over PDAs (Personal Digital Assistants), mobile phones and other network devices, over public channels (cable, satellite, wireless networks, Internet, etc.) [6]. Naturally one main concern is copyright protection and access control.

To protect copyright and access control, broadcaster should use an encryption system [1] [6]. However, the limited batteries life of these devices obliges to reduce encryption computational complexity. Furthermore, access control mechanisms can enforce security protecting mainly confidentiality and integrity – availability is not addressed here, despite its importance, since it is normally enforced by different controls. Standard cryptographic techniques can guarantee high level of security but at the cost of expensive implementation and important transmission delays [11]. Selective encryption comes as an alternative that aims to provide sufficient security with an important gain in computational complexity and delays [1].

Broadcasting Encryption (BE) aims to distribute the data to all authorized users simultaneously, in an efficient way and securely [15]. This balance is particularly critical with small devices which don't have enough resources to implement complex encryption techniques. Furthermore, this devices usually do not even keep information between sessions – stateless devices. Within stateless receivers, a media server must deliver information securely to the authorized users over a public channel, where the receivers do not update their state from session to session [13].

A typical CAS (Conditional Access System) depends on three level of encryption as shown in Fig. 1; at the sender side, the raw content is encrypted using a Control Word (CW), which is encrypted by a Service Key (SK). SK is embedded into an Entitlement Control Message (ECM), which is encrypted using a Personal Distribution Key (PDK) assigned to each authorized user. The PDK is embedded into an Entitlement Management Message (EMM). The EMM is specific to each subscriber, as identified by the smart card in their receivers, or to groups of subscribers, and are issued much less frequently than ECMs, usually by monthly intervals. Encrypted content (both ECM and EMM) is transmitted through broadcast networks. SK is renewed at intervals of hours or days, while PDK is static and known only by the service provider and the user's terminal, being embedded into firmware. At the receiver side, SK is decrypted and used to decrypt ECM, which allows getting CW, necessary to decrypt the content [14]. For pay TV, many authors preferred building a separate key tree for each multicasting program [10].

As stated above, considering low power receivers, the cipher system should be both robust and low demanding, considering computational resources. The mechanism proposed in this paper tries to respond to those requirements.

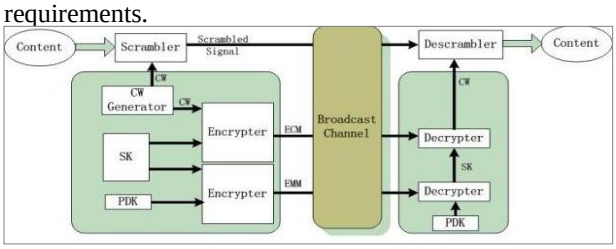

Figure 1. typical Conditional Access System [14].

 ISBN: 978-1-61208-195-3

This paper is organized as following: in section II we overview the related work; in section III, we present our approach, and conclude in section IV.

II. LITERATURE REVIEW

Eagle et al. [5] studied the number of encryption operations necessary to revoke keys. They studied the well-known used trees based broadcast encryption schemes. They proved that the mean number of encryption processes for the complete sub-tree scheme and the subset-difference scheme studied by previous studies were good estimates for the number of encryption processes used by this scheme. Their study focused on proving a normal limiting distribution for the number of encryptions as the number of users became large. They took into consideration the combined number of encryptions and number of privileged users in a random privileged set [5].

In [4], Kirkels et al. described a security architecture for a pay-TV CAS. They focused on the design constraints related to a conditional access client in the design of the architecture and maximum amount of bandwidth available for the transmission of conditional access messages. They presented the design and analysis of their efficient injector model based on queuing theory, conditional access messages into the broadcast stream. To demonstrate the effectiveness of the presented approach, they presented a numerical example with real-world values.

In [1], Massoudi et al. introduced the selection encryption of image and video scheme to reduce the amount of encrypted data, keeping the security goals. Their protocol consists of two parts: public part, where there is no encryption; and protected part, encrypted and only accessible to authorized users.

In [14], Zhang et al. introduced a novel way to solve the tradeoff problem about communication, storage and computation overhead of BE scheme. They suggested getting rid of the computation overhead that come from broadcast key generation. They constructed a scheme based on Subset Difference (SD) and RSA accumulator. Their idea of separating the user-side device into two different function parts (private and public parts), taking advantage of the public device's functionality, minimize the storage and computation overhead of the private device, and make BE scheme more implementation-oriented.

In [9], Shirazi et al. presented and described Mobile Integrated Conditional Access System (MICAS). They demonstrated the various architectures to deliver key information at an arbitrary located device, at the surrounding area of the subscriber. They described the advantages of the system. Their proposed system included the message handling subsystem with a so-called 'Follow-Me' service, which extends mobility and personalization concepts on pay-TV services. Subscriber Management and Subscriber Authentication Subsystems would respond to the subscribers interaction (via mobile phone) issuing them the corresponding access rights. Their system is supposed to reduce the cost for service provider and end-users by respectively cutting down the service deployment cost and eliminating the requirement of additional receiver as changing the service provider.

Abdalla et al. [10] discussed how to communicate securely with a set of users (the target set) over an insecure broadcast channel for application domains: satellite/cable pay TV and the Internet MBone. They concerned about the number of key transmissions and the number of keys held by each receiver. They suggested maintaining single key structure such that receiver should keep a logarithm number of establishment keys, for the entire life time [10].

Zhang et al. [14] presented a CAS model using an encryption scheme for one way broadcasting and protection application. They compared it with traditional Conditional Access Systems. They discussed the advantages and challenges of BE [14].

In [8], Koo et al. presented a key refreshment management scheme for CAS in DTV broadcasting. They concluded that their scheme perform dynamic entitlement management securely and efficiently and reduced a key generation and encryption load for CAS. In [7], authors discussed the problem of a server sending a message to a group of the stateless receivers, assuming that a subset of the keys have been revoked and should not be able to obtain the content of the message. They provided sufficient conditions to guarantee the security of revocation schemes.

In [13], Hwang et al. presented an efficient revocation scheme for stateless receivers. They used a logical hierarchical key tree. They considered Asano's schemes [12] very efficient with respect to key storage. They used hierarchical key based on a binary tree, and they found that it requires the same message length as the SD scheme. Asano proposed two efficient revocation methods for stateless receivers. He used the Master Key technique and the 'Power Set Method' with an a-ary key tree structure in order to reduce the number of keys each receiver stores and the number of ciphered messages broadcasted, respectively. The first method required receivers to store only one key. The second method was supposed to reduce the computational overhead imposed to receivers, but with an increase in the number of master keys they have to store. He discussed the security of his methods and some techniques used in his methods [12].

In spite of all the work already done, key management is still a main concern in multimedia CAS, particularly considering small devices with computational resource constraints and real-time demands. Key exchange and revocation must be very efficient tasks in order to achieve fast and low power consummation operations. None of the previous solutions seems to be an optimal solution, justifying additional research efforts.

III. PROPOSED SYSTEM

The approach proposed in this paper aims at protect copyright, without requiring substantial architecture modifications, and avoiding the need to store or exchange encryption keys; every block is encrypted using a different schedule key, which is scrambled within the message

The proposed protocol assumes that:

 ISBN: 978-1-61208-195-3

1. Registration: users should register and would be granted the personal distribution key (PDK) – this distribution mechanism is not a main concern here.
2. Compression: raw content would be compressed.
3. Private Cipher key (CK) generation: key is generated and expanded to gain schedule key.
4. Encryption: expanded CK is used to encrypt the compressed raw data.
5. Scramble: both CK and encrypted data (C) are transmitted together in a scrambled way.
6. Broadcasting the cipher key can be solved by scrambling the cipher key with ciphered block in a special way that only the legitimated receiver can understand, allowing it to extract both cipher key and ciphered block and this way decypher the original message. The scrambling technique is described next.

A. *Scrambling Algorithm: Starting Random*

First, a Boolean number is randomly generated. A zero means to start with the ciphered data block element, whereas a one implies starting with ciphering key, as shown in Fig. 2. After that, the scrambling process proceeds according to the algorithm presented in the listing bellow, for which an output example is given in Fig. 3, and a flowchart is given in Fig. 4.

Scrambling Algorithm
Input: ciphered data block, ciphering key
Output: Scrambled Token (ST).
Function Scrambling
Begin
Generate start, using lookup table
for i=0 to block Cipher size-1 step by 1
ST 2i+1+ start += ciphered data block i
ST 2i+ start += ciphering key block i
end for
ST= the rest of the ciphering key
end function Scrambling

1) *Illustrative Example Using AES algorithm*

To illustrate how the algorithm works we will show next an example for a symmetric block ciphering (e.g., AES). Assuming Nb represents the block length in bytes (C0-C15), 16 bytes in this example. The ciphering key should be the same length, denoted by Ck0 -Ck15.

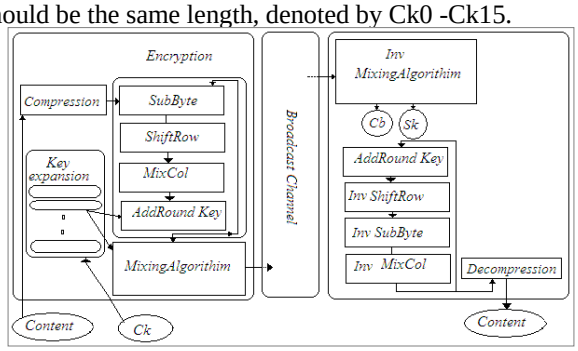

Figure 2. Proposed System

0	1	2	3	4	5
0	C_0	Ck_0	C_1	Ck_1	C_2
6	7	8	9	10	11
Ck_2	C_3	Ck_3	C_4	Ck_4	C_5
12	13	14	15	16	17
Ck_5	C_6	Ck_6	C_7	Ck_7	C_8
18	19	20	21	22	23
Ck_8	C_9	Ck_9	C_{10}	Ck_{10}	C_{11}
24	25	26	27	28	29
Ck_{11}	C_{12}	Ck_{12}	C_{13}	Ck_{13}	C_{14}
30	31	32			
Ck_{14}	C_{15}	Ck_{15}			

Figure 3. Ciphered block and ciphering key

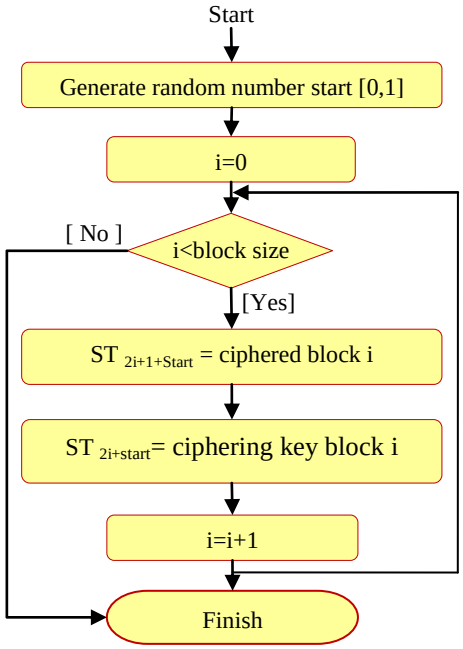

Figure 4. Proposed Algorithm

Following the algorithm proposed, in this case the output would be 33 bytes long, comprising one byte start code, 16 bytes for ciphered data and 16 bytes for cipher key.

Assuming the ciphered data block was: “a6 d9 f3 60 39 53 ff 11 13 6e 03 06 7f 8a 57 fa”, as shown in Fig. 5 and the ciphering key was “41 73 69 6d 20 41 20 45 6c 2d 53 68 65 69 6b 68”, as shown in Fig. 6, and assuming the random generator produced a 0 start code, the output block would be filled starting with ciphered data and will look like the stream showed in Fig. 7.

 ISBN: 978-1-61208-195-3

a6	d9	f3	60
39	53	ff	11
13	6e	03	06
7f	8a	57	fa

Figure 5. Ciphered block

a6	d9	f3	60
39	53	ff	11
13	6e	03	06
7f	8a	57	fa

Figure 6. Ciphered block

0	1	2	3	4	5
0	**a6**	41	**d9**	73	**f3**
6	7	8	9	10	11
69	**60**	6d	**39**	20	**53**
12	13	14	15	16	17
41	**ff**	20	**11**	45	**13**
18	19	20	21	22	23
6c	**6e**	2d	**03**	53	**06**
24	25	26	27	28	29
68	**7f**	65	**8a**	69	**57**
30	31	32			
6b	**fa**	68			

Figure 7. Output of mixing ciphered block & ciphering key

IV. CONCLUSION

This paper introduced a new approach for multimedia Conditional Access Systems (CAS), avoiding the key exchange scheme. This technique is particularly useful for stateless receivers. The proposed approach uses dynamic key generation. Our approach is efficient with respect of the number of keys stored and used to encrypt the data. It reduces the complexity of other solutions as it does not need to encrypt the ciphering keys. It uses fewer keys to reduce the storage and scramble the transmitted data to reduce encrypting the keys. Furthermore, the presented approach eliminates the proposed key refreshment presented in [14] and [8]. However, there will provide a gain in computational complexity and delays. We demonstrated how the proposed technique works using a block cipher like AES, proposed by [3]. A practical example is used to demonstrate the effectiveness of the presented approach.

As future work, we will demonstrate a practical architecture and evaluate the resistance to direct attacks. For future, we will test the algorithm in real CAS environment (IPTV system) to compare it with well-known algorithms. The comparison with similar work in the real systems would be reflected by the benefits that algorithm would introduce to the industry.

ACKNOWLEDGMENT

This work was funded by FEDER through Programa Operacional Fatores de Competitividade – COMPETE, and by national founds through FCT – Fundação para a Ciência e Tecnologia, under project: FCOMP-01-0124-FEDER-022674.

REFERENCES

[1] A. Massoudi, F. Lefebvre, C. De Vleeschouwer, B. Macq, and J. Quisquater (2008), “Overview on Selective Encryption of Image and Video: Challenges and Perspectives”, EURASIP Journal on Information Security, Vol. 2008, (January 2008), Article 5.

[2] A. Rashed (2007), “Using Modified Genetic Algorithm to Replace AES Key Expansion Algorithms”, The International Conference on Information Technology (ICIT’2007) at Al-Zaytoonah University, Jordan on May 9-11, 2007. WWW.alzaytoonah.edu.jo/icit2007

[3] A. Rashed and N. Ajlouni (2004), “An Extended Rijndael Block Cipher Using Java”, the 2004 International Conference on software Engineering Research and practice, Las Vigas, Nevada USA, June 2004, pp. 21-24.

[4] B. Kirkels, M. Maas, and P. Roelse (2007), ”A Security Architecture for Pay-Per-View Business Models in Conditional Access Systems”, ACM Workshop On Digital Rights Management, Proceedings of the 2007 ACM workshop on Digital Rights Management: Alexandria, Virginia, USA:1-9.

[5] C. Eagle, Z. Gao, M. Omar, D. Panario, and B. Richmond (2008), “Distribution of the Number of Encryptions in Revocation Schemes for Stateless Receivers”, Fifth Colloquium and Computer Science, DMTCS proc. AI: pp. 195-206.

[6] D. Dardari, M. Martini., M. Mazzott, and M. Chiani (2004), “Layered Video Transmission on Adaptive OFDM Wireless Systems”, EURASIP Journal on Applied Signal Processing, Volume 2004: pp. 1557 - 1567

[7] D. Naor, M. Naor, and J. Lotspeich (2001), “Revoking and Tracing Scheme of Stateless Receiver”, Proceedings of Crypto01, LNCS 2139, pp. 29-30.

[8] H. Koo, O. Kwon, and J. Kim (2005), “Key Refreshment Management for Conditional Access System in DTV Broadcasting”, International Conference consumer Electronics, Jan 2005 : pp. 29-30

[9] H. Shirazi, J. Cosmas, D. Cutts, N. Birch, and P. Daly (2008), “Security Architectures in Mobile Integrated Pay-TV Conditional Access System”, Networks 2008 - 13th International Telecommunications Network Strategy and Planning Symposium 1.

[10] M. Abdalla, Y. Shavitt, and A. Wool (2000), “Key Management for Restricted Multicast Using Broadcast Encryption”, IEEE/ACM Transactions on Networking (TON), Vol. 8 , Issue 4: pp. 443 - 454

[11] N. Ajlouni, A. El-Sheikh, and A. Rashed (2006), “New Approach in Key Generation and Expansion in Rijndael Algorithm”,

 ISBN: 978-1-61208-195-3

International Arab Journal of Information Technology, vol. 3, no. 1, January 2006.

[12] T. Asano (2002), "A Revocation Scheme with Minimal Storage at Receivers", ASIACRYPT'02, LNCS V.2501: pp. 433-450.

[13] Y. Hwang, H. Chong, and J. Pil (2004), "An Efficient Revocation Scheme for Stateless Receivers", EuroPKI 2004, LNCS 3093, Springer-Verlag Berlin Heidelberg: pp. 322–334.

[14] Y. Zhang, C. Yang, J. Liu, and J. Tian (2009), "Broadcast Encryption Scheme and Its Implementation on Conditional Access System", Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09) Nanchang, P. R. China, May 22-24, 2009: pp. 379-382

[15] Y. Zhang, C. Yangt, J. Liu, and J. Li (2007), "A Novel Broadcast Encryption Scheme Based on SD Scheme Reconstruction", Communications and Networking in China, 2007. CHINACOM '07, Second International Conference on Digital Object Identifier: 10.1109/CHINACOM.2007.4469408, pp.: 387 – 391.

 ISBN: 978-1-61208-195-3