RAPPORT 1079-1

CARACTÉRISTIQUES GÉNÉRALES D'UN SYSTÈME DE RADIODIFFUSION A ACCÈS CONDITIONNEL

(Question 37/11)

(1986-1990)

1. Introduction

Le présent Rapport contient les principes des systèmes à accès conditionnel élaborés par l'UER en vue de leur application à la télévision par satellite, et également par la France et le Royaume-Uni, où les principes ont été appliqués aux services de télétexte. Certains détails de ces applications sont réunis dans le Tableau I figurant à la fin du présent Rapport.

Ces principes peuvent également s'appliquer aux systèmes classiques de radiodiffusion sonore et télévisuelle ainsi qu'aux services supplémentaires autres que le télétexte qui sont énumérés dans le Rapport 802.

2. Eléments d'un système à accès conditionnel

Il existe deux éléments distincts, et souvent indépendants:

2.1 *L'embrouillage**

Il consiste à rendre un service inutilisable aux usagers non autorisés en modifiant certaines de ses caractéristiques sous le contrôle du système d'accès conditionnel à l'émission.

2.2 *Le contrôle d'accès**

Il consiste à fournir des informations permettant aux usagers autorisés de désembrouiller le service. On contrôle l'utilisation de ces informations en les transmettant sous forme chiffrée*.

3. Propriétés attendues d'un système à accès conditionnel

3.1 *Sécurité*

La sécurité du système est le degré de difficulté rencontré par un usager non autorisé lorsqu'il tente d'accéder aux services.

Les deux aspects suivants sont à distinguer:

- le désembrouillage du signal sans référence au processus de contrôle d'accès; cette fraude dépend de la nature des services et de la méthode d'embrouillage;
- l'obtention illicite de la clé* de contrôle d'accès. Cette fraude dépend de la sécurité des algorithmes utilisés et de la méthode de distribution des clés.

---

* Voir l'Annexe I pour les définitions.

3.2 *Modes d'accès*

Un système à accès conditionnel est plus efficace s'il comporte plusieurs modes d'accès.

Les modes d'accès peuvent être, par exemple:

- l'abonnement à la période – l'autorisation est accordée entre une date initiale et une date d'expiration;
- la taxation à la séance – l'accès au service est autorisé pour une session donnée, que cette session soit complètement utilisée ou non;
- la taxation à la consommation – la taxe, ou l'imputation, est proportionnelle à la durée d'utilisation et/ou à la valeur du service concerné.

Les modes d'accès doivent varier en fonction de plusieurs paramètres, par exemple:

- le temps,
- différents segments du service,
- des groupes d'usagers particuliers.

3.3 *Normalisation des équipements*

La normalisation permet de fabriquer le plus économiquement possible des équipements de réception et d'en simplifier la gestion et la maintenance:

- les équipements communs devraient être normalisés pour que ceux-ci puissent s'adapter à une quantité d'options de service aussi importante que possible;
- les éléments «secrets» devraient être abrités dans un module sûr, équipé d'une interface normalisée* .

3.4 *Gestion de l'accès*

La définition de l'accès conditionnel est fondée sur la notion de *titre* d'accès, et celui-ci peut se présenter sous différentes formes. En vertu de son titre d'accès, un usager dispose d'une *autorisation* d'accès au service correspondant.

3.5 *Moyens d'éviter les dégradations du service*

Il existe trois catégories de dégradations importantes:

- les dégradations affectant le service offert qui sont dues aux processus d'embrouillage/de désembrouillage;
- les dégradations dues à une acquisition défectueuse ou non fiable des données de contrôle d'accès;
- l'utilisation non économique des ressources due aux opérations de gestion et de transmission de ces mêmes données.

3.6 *Interaction avec le traitement numérique*

Il convient de noter qu'il existe des processus d'embrouillage incompatibles avec certaines opérations relatives aux techniques de traitement numérique des signaux dont, par exemple, les techniques de réduction du débit binaire.

4. Description générale d'un système à accès conditionnel

4.1 *Généralités*

Dans un système à accès conditionnel, l'information doit être *embrouillée* avant sa diffusion. Le processus d'embrouillage est placé sous le contrôle de la séquence d'embrouillage obtenue à partir d'un *générateur pseudo-aléatoire.*

Pour le processus de désembrouillage à la réception, il faut utiliser la même séquence (séquence de désembrouillage dans ce cas) afin de régénérer le signal d'origine.

---

* Cette question a déjà été traitée à l'UER en liaison avec les spécifications relatives à un système direct de radiodiffusion par satellite (SRS) à accès conditionnel (voir le Rapport 1073).

En vue de fournir cette séquence et d'assurer la synchronisation entre les processus qui interviennent à l'émission et à la réception, on utilise un *mot d'initialisation* pour contrôler les conditions initiales du générateur pseudo-aléatoire du train de bits.

Pour assurer la sécurité du système, l'information relative à l'accès et permettant de récupérer le mot d'initialisation est transmise sous forme chiffrée et en accord avec les modes d'accès utilisés (voir la Fig. 1). La structure détaillée de ce processus est décrite dans la Fig. 2 et dans la suite du texte.

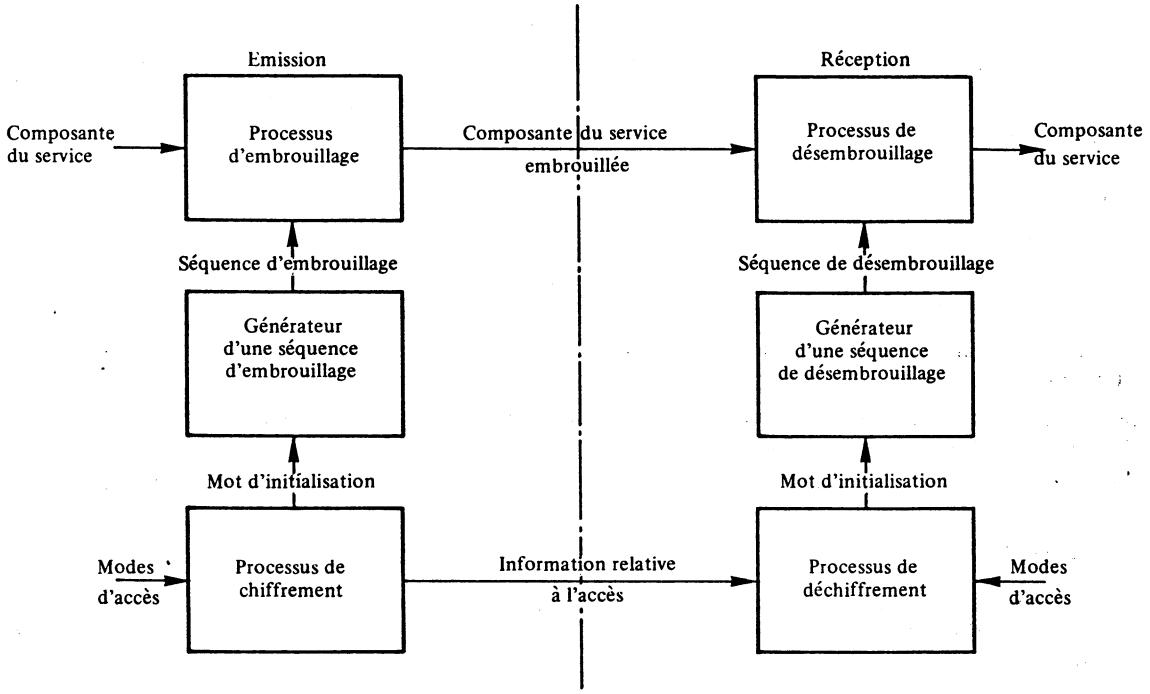


FIGURE 1 – *Système de base à accès conditionnel*

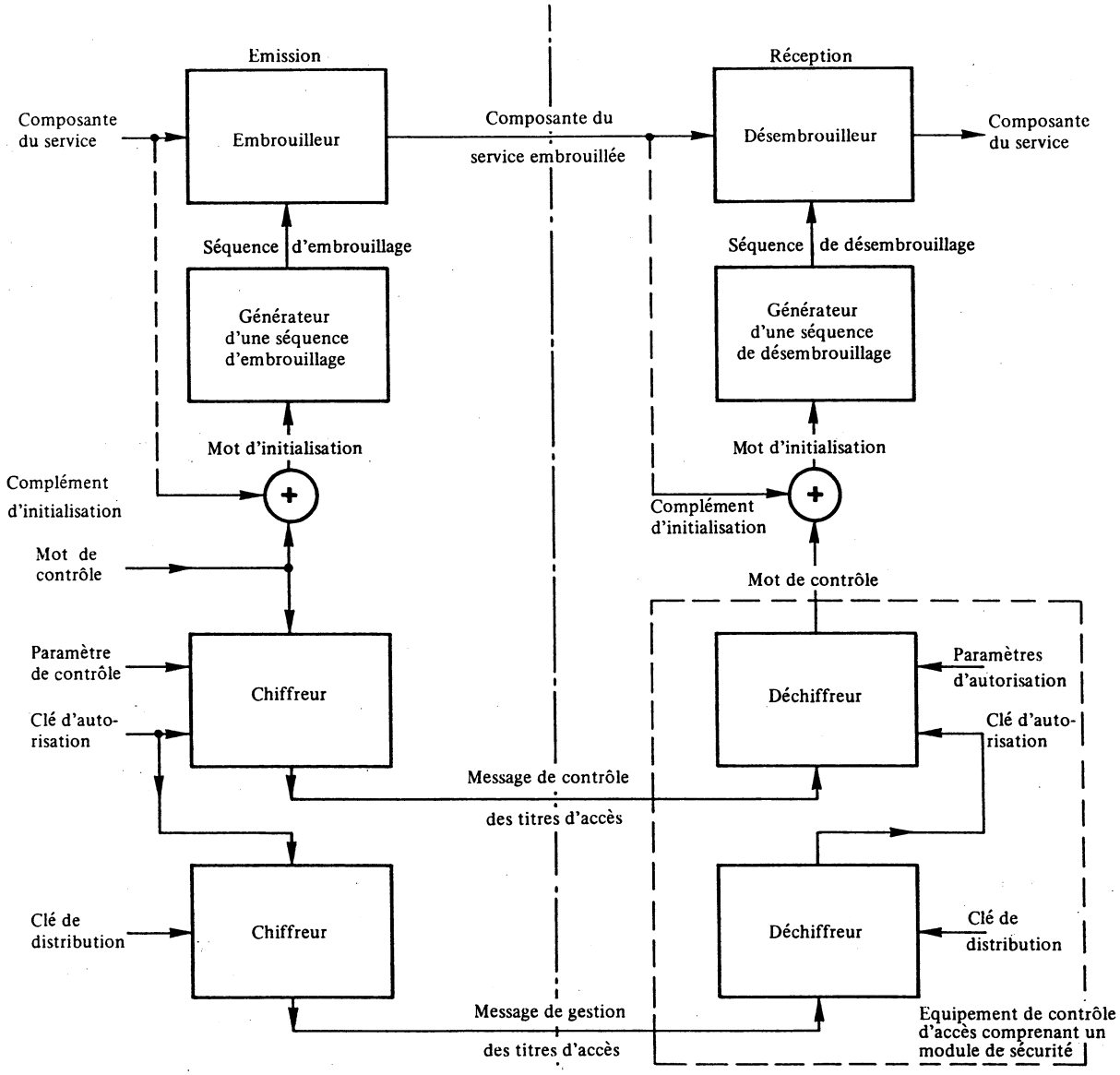


FIGURE 2 – *Description fonctionnelle d'un système de radiodiffusion à accès conditionnel*

Note. – Deux chiffreurs et déchiffreurs sont représentés sur cette figure dans un souci de clarté. En pratique, 1 chiffreur et 1 déchiffreur peuvent suffire si l'algorithme de chiffrement commandé par la clé d'autorisation et celui qui est commandé par la clé de distribution sont identiques.

4.2 *Mot d'initialisation*

L'accès conditionnel à une composante d'un service est en fait, équivalent à l'accès conditionnel au mot d'initialisation qui est composé des deux éléments suivants: le *mot de contrôle* et le *complément d'initialisation.*

4.3 *Mot de contrôle*

Le mot de contrôle est l'élément de base de la sécurité. Sa valeur est choisie arbitrairement et peut être modifiée pendant l'exploitation du service pour améliorer la sécurité.

Le mot de contrôle est communiqué au récepteur comme suit:

- à l'émission, suivant le mode d'accès utilisé, un algorithme de chiffrement donne des versions chiffrées du mot de contrôle, qui sont transmises dans des entités particulières, que l'on appelle les *messages de contrôle des titres d'accès*;
- à la réception, l'équipement de contrôle d'accès utilise l'algorithme inverse pour restituer le mot de contrôle.

4.4 *Complément d'initialisation*

Le complément d'initialisation est utilisé pour imposer des séquences d'embrouillage suffisamment brèves permettant d'assurer la sécurité tout en évitant de procéder à des calculs trop fréquents du mot de contrôle. Ainsi, l'utilisation de différents compléments d'initialisation pour chaque unité structurelle de l'information embrouillée permet de modifier de façon suffisamment fréquente le mot d'initialisation.

4.5 *Indice de mot de contrôle*

Pour réaliser la segmentation d'un service, il est nécessaire de gérer plusieurs mots de contrôle associés aux différents segments du service. On identifie ces mots au moyen d'*indices.* L'indice du mot de contrôle utilisé pour accéder à une unité d'information embrouillée doit pouvoir être obtenu à partir du signal transmis.

5. Messages de contrôle des titres d'accès

Chacun de ces messages comprend les éléments suivants:

- l'indice du mot de contrôle;
- un drapeau de modification du mot de contrôle: un changement d'état indique un changement de valeur du mot de contrôle;
- un *pointeur d'autorisation* qui identifie la clé d'autorisation située dans le module de sécurité du récepteur auquel le message est adressé;
- un *paramètre de contrôle* qui fournit des valeurs (par exemple, date, prix, etc.) destinées à être comparées aux limites qui leur sont fixées dans le module de sécurité du récepteur et que l'on appelle *paramètres d'autorisation*;
- le mot de contrôle chiffré.

Pour désembrouiller une unité d'information, le récepteur doit d'abord avoir extrait le mot de contrôle d'un message de contrôle des titres d'accès portant l'indice approprié.

Afin d'obtenir une efficacité optimale, il convient de regrouper sous le même indice les messages de contrôle des titres d'accès relatifs au même mot de contrôle mais correspondant soit à différents identificateurs d'audiences soit à différents types d'équipement de contrôle d'accès. Bien que ce ne soit pas sa seule application, le système d'indiçage décrit ci-dessus permet de réaliser la transmission anticipée des messages de contrôle des titres d'accès.

L'équipement d'accès conditionnel crée une table des mots de contrôle actifs, mise à jour par les messages de contrôle des titres d'accès indépendamment des données embrouillées. Pour identifier le mot de contrôle des titres correct, le dispositif de désembrouillage fournit à l'équipement de contrôle d'accès l'indice correspondant. La gestion de cette table fait partie intégrante des fonctions assurées à l'interface entre le désembrouilleur et l'équipement de contrôle d'accès.

6. Messages de gestion des titres d'accès

Le traitement d'un message de gestion des titres d'accès permet de valider ou d'acquérir le titre d'accès. Ce processus intervient dans le module de sécurité associé à un calcul cryptographique faisant intervenir une *clé de distribution.* La clé de distribution est utilisée pour chiffrer et déchiffrer des messages et/ou des clés d'autorisation adressées à des récepteurs individuels. Les cryptogrammes correspondants constituent le signal de validation et sont acheminés à l'intérieur des messages de gestion des titres d'accès.

Dans les systèmes de radiodiffusion à accès conditionnel, les messages de gestion des titres d'accès peuvent être radiodiffusés. C'est ce que l'on appelle l'adressage sur antenne. On peut réduire sensiblement la durée du cycle associé à la distribution des clés sur antenne en appliquant les principes des systèmes de chiffrement à clef partagée (voir la section 2 de l'Annexe II). Les messages de gestion des titres d'accès peuvent également être diffusés par d'autres médias.

En cas de paiement par unité de temps ou par programme, les messages de gestion communiquent un code de coûts chiffré, qui est transmis dans le cadre du service offert. Le crédit stocké dans le récepteur peut revêtir la forme de jetons de sommes d'argent chiffrés qui sont transmis dans le cadre d'un service d'adressage sur antenne (voir la section 3 de l'Annexe II). Le crédit peut également prendre la forme de jetons de sommes d'argent stockés, qui sont distribués par d'autres moyens. Le paiement consiste à diminuer le crédit enregistré en fonction du code de coût reçu.

7. Equipement de contrôle d'accès

Cet équipement comprend notamment un module de sécurité qui reçoit les messages de contrôle des titres d'accès. Le module peut être fixe ou amovible (par exemple, carte à mémoire). L'équipement de contrôle d'accès communique avec le désembrouilleur par l'intermédiaire d'une interface physique et de circuits logiques. La normalisation de cette interface est importante, car elle permet de préserver:

- l'indépendance du module de sécurité et de la fonction de désembrouillage intégrée au récepteur;
- le développement ultérieur de l'équipement de contrôle d'accès.

Si le module de sécurité contient une autorisation avec le même identificateur que le pointeur d'autorisation figurant dans le message de contrôle des titres d'accès, il fournit un mot de contrôle si, en outre, les paramètres de contrôle remplissent les conditions du paramètre d'autorisation. Parmi ces conditions, on peut trouver notamment:

- une condition de date, la date figurant dans le paramètre de contrôle devant être comprise entre les dates de départ et d'expiration du paramètre d'autorisation;
- une condition de coût qui permet à une autorisation d'être délivrée seulement si un débit de taxes est accepté par le module de sécurité.

Une transaction faisant intervenir le module de sécurité peut se diviser en trois étapes:

- instructions préliminaires, le cas échéant (par exemple, mot de passe, consentement de l'usager, etc.);
- instructions d'exploitation utilisant le module de sécurité;
- traitement (par exemple, délivrance du mot de contrôle).

Comme divers modules de sécurité peuvent être utilisés, il serait souhaitable que l'équipement de contrôle d'accès soit indépendant des transactions spécifiques. Cette indépendance peut être obtenue si l'équipement de contrôle d'accès sait interpréter une séquence d'instructions traduites dans un langage spécifique et transmise dans des messages particuliers.

8. Applications

Les techniques à accès conditionnel ont été appliquées à certains systèmes de télétexte ———— organisés par pages et à l'utilisation de systèmes de radiodiffusion de données indépendants (voir la Recommandation 653), ———— aux systèmes de radiodiffusion par satellite (voir le Rapport 1073) et aux systèmes de radiodiffusion de Terre (voir le Rapport 802). Quelques exemples sont donnés dans le Tableau I.

TABLEAU I – *Exemples de mise en œuvre d'un système à accès conditionnel*

Référence à ce Rapport	Systèmes de télétexte organisés par page		Systèmes de radiodiffusion de données		Famille MAC/paquets (Rapport 1073, C-MAC/paquets et D2-MAC/paquets)
	Télétexte système A [CCIR, 1982-86, Partie I, Chapitre 5]	Télétexte système B [CCIR, 1982-86, Partie II]	Lignes avec données indépendantes Télétexte système B	Couches 1 à 4 du Télétexte système C adopté en France	
Processus d'embrouillage § 4.1	Combinaison par un OU-exclusif d'octets de données avec les octets d'un générateur pseudo-aléatoire. Un octet d'interprétation dans l'en-tête indique si l'article est embrouillé ou non. Voir le § 3.1.	Combinaison par un OU-exclusif des octets de données avec les octets d'un générateur pseudo-aléatoire. Les liaisons du paquet 27 indiquent que la page est embrouillée. Voir le § 20.1.	Combinaison par un OU-exclusif d'octets de données avec les octets d'un générateur de trains de données d'embrouillage L'apparition régulière de blocs de clés de données d'utilisateur indique que le service est embrouillé	Combinaison par un OU-exclusif d'octets de données avec les octets d'un générateur pseudo-aléatoire. Dans le complément d'initialisation, un octet indique si le groupe de données est ou non embrouillé. Les groupes de données où GT = 0 ou 1 ne sont pas embrouillés.	*Image:* rotation de composante à double coupure ou rotation de ligne à simple coupure, sous le contrôle d'un générateur pseudo-aléatoire. *Son:* combinaison par un OU-exclusif bit par bit des bits de données avec les bits d'un générateur pseudo-aléatoire fonctionnant en continu.
Générateur pseudo-aléatoire § 4.1	Combinaison de trois registres à décalage multi-étages à rétroaction linéaire. Voir l'Annexe I.	Utilisation d'une fonction unidirectionnelle employant un algorithme à rétroaction de chiffrement. Voir les notes du § 20.	Le générateur de trains d'embrouillage utilise un algorithme de chiffrement connecté en mode de sortie à rétroaction (ISO DIS 8372).	Combinaison de trois registres à décalage multi-étages à rétroaction linéaire.	*Image:* deux registres à décalage multi-étages à rétroaction linéaire. *Son:* deux registres à décalage multi-étages à rétroaction linéaire initialisant un autre registre à décalage multi-étages à rétroaction linéaire.
Synchronisation du générateur pseudo-aléatoire § 4.1	Premier octet suivant la première séquence US-X-Y de l'article. Voir le § 2.3.	Premier octet de données du paquet 0 d'une page désignée. Voir le § 20.	Le premier octet des données d'utilisateur se trouve dans le bloc de données d'utilisateur	Premier octet suivant le complément d'initialisation.	Au départ de chaque trame.
Mot d'initialisation § 4.2	12 octets. Voir le § 2.3.	Clé de page de 56 bits. Voir le § 20.1.	La variable initiale du train d'embrouillage est un octet unique au départ du bloc de données d'utilisateur, répété 8 fois	12 octets.	60 bits.
Mot de contrôle § 4.3	8 octets aléatoires. Voir le § 2.1.	Clé (56 bits) du système en vigueur. Voir le § 20.1.3.	Clé d'utilisateur de 64 bits.	8 octets aléatoires.	60 bits, soit choisis de manière aléatoire soit sous forme de cryptogramme du compteur de 256 trames.
Complément d'initialisation § 4.4	4 octets suivant l'en-tête du message. Voir le § 2.3.	Ne s'applique pas.	Ne s'applique pas.	4 octets suivant l'en-tête du groupe de données.	La valeur du compteur de trames à 8 bits.

TABLEAU I (suite)

Référence à ce Rapport	Systèmes de télétexte organisés par page		Systèmes de radiodiffusion de données		Famille MAC/paquets (Rapport 1073, C-MAC/paquets et D2-MAC/paquets)
	Télétexte système A [CCIR, 1982-86, Partie I, Chapitre 5]	Télétexte système B [CCIR, 1982-86, Partie II]	Lignes avec données indépendantes Télétexte système B	Couches 1 à 4 du Télétexte système C adopté en France	
Message de contrôle des titres d'accès § 5	Articles désignés avec pour numéro de classification FFF et $Y_{11} = 1$; l'octet Y_{12} donne l'indice du mot de contrôle. Chaque message est introduit par la séquence US-3/F-3/F et comprend: – 3 octets pour le pointeur d'autorisation – 3 octets pour le paramètre de contrôle – 16 octets pour le mot de contrôle chiffré. Voir le § 3.2.	Les paquets désignés comprennent des paramètres d'autorisation et de contrôle à 22 bits et un mot de contrôle chiffré de 112 bits. Voir le § 20.1.3.	Un type de bloc de contrôle transmet une clé de données d'utilisateur à tous les utilisateurs disposant d'une clé de système valable leur permettant de la déchiffrer.	Groupes de données pour lesquels GT (type du groupe de données, voir Recommandation 653, Tableau Ia, point 4.1) est égal à 14. Les groupes de données sont constitués d'ordres, chaque ordre étant identifié par un identificateur d'ordre et un identificateur de longueur d'ordre, et composé de paramètres identifiés par un identificateur de paramètre et un identificateur de longueur de paramètre; on définit deux types d'ordre: CI = 0: référence du module de sécurité à utiliser; CI ≠ 0: ordre de contrôle des titres d'accès, où chaque paramètre transporte un ECM et comprend: - 3 octets pour l'impression de l'autorisation, - 3 octets pour le paramètre de contrôle, - 16 octets pour le mot de contrôle chiffré.	Paquets désignés dans la voie d'identification du service. Pour le système d'accès conditionnel pour les services diffusés en D2-MAC/paquet, qu'utilise notamment le système français de radiodiffusion directe par satellite TDF1-TDF2, le codage de ces paquets est conforme aux dispositions de la spécification "Système d'accès conditionnel pour la famille MAC/paquet EUROCRYPT" (mars 1989) [CCIR, 1986-90a]. Au Royaume-Uni, où le système D-MAC/paquet a été adopté, le service de radiodiffusion par satellite britannique commencera l'exploitation du SRS en utilisant le système d'accès conditionnel Eurocypher [CCIR, 1986-90b].
Indice de mot de contrôle § 4.5	Octet Y_{16} de l'article embrouillé pour le désembrouillage et octet Y_{12} du message de contrôle de titre d'accès pour mise à jour. Voir les § 3.1 et 3.2.	Ne s'applique pas.	Ne s'applique pas.		Ne s'applique pas.
Changement de mot de contrôle et de drapeau § 5	Bit b_x de l'octet Y_{12} du message de contrôle de titre d'accès. Voir le § 3.2.	Mots clés en vigueur et nouveaux inclus dans un paquet désigné de la page d'adressage à l'utilisateur. Voir le § 20.2.	On identifie les versions correctes des clés en mettant en correspondance les clés d'étiquette transmises avec les clés et avec les blocs de données pour lesquels ces clés sont nécessaires.	Bit b_8 de l'identificateur de paramètre de l'ordre de contrôle des titres d'accès	Un nouveau mot de contrôle est transmis toutes les 256 trames et devient le mot de contrôle en vigueur lorsque le comptage de trames atteint zéro.

TABLEAU I (suite)

Référence à ce Rapport	Systèmes de télétexte organisés par page		Systèmes de radiodiffusion de données		Famille MAC/paquets (Rapport 1073, C-MAC/paquets et D2-MAC/paquets)
	Télétexte système A [CCIR, 1982-86, Partie I, Chapitre 5]	Télétexte système B [CCIR, 1982-86, Partie II]	Lignes avec données indépendantes Télétexte système B	Couches 1 à 4 du Télétexte système C adopté en France	
Message de gestion des titres d'accès § 6	Le titre d'accès est actuellement géré par un système vidéotex sur un réseau de télécommunications. Voir le § 1.3.	Le titre d'accès est géré par adressage sur antenne de l'équipement d'utilisateur au moyen de paquets d'adressage d'utilisateur en partage et d'utilisateur unique. Voir le § 20.2.	Le titre d'accès est géré par adressage sur antenne du module de contrôle d'accès au moyen de blocs de données d'adressage d'utilisateur en partage et d'utilisateur unique. Les blocs de données pour adressage sur antenne sont multiplexés dans la même voie sous forme de données de message.	Pas encore normalisé. Les titres d'accès peuvent être gérés par un système de vidéotex sur un réseau de télécommunications.	Paquets désignés dans la voie SI. Pour le système d'accès conditionnel aux services diffusés en D2-MAC/paquet, qu'utilise notamment le système français de radiodiffusion directe par satellite TDF1-TDF2, le codage de ces paquets est conforme aux dispositions de la spécification "Système d'accès conditionnel pour la famille MAC/paquets EUROCRYPT" (mars 1989) [CCIR, 1986-90a]. Au Royaume-Uni, où le système D-MAC/paquet a été adopté le service de radiodiffusion par satellite britannique commencera l'exploitation du SRS en utilisant le système d'accès conditionnel Eurocypher [CCIR, 1986-90b].
Equipement de contrôle d'accès § 7	Incorporé dans le récepteur et comportant un lecteur de carte à mémoire. Voir le § 1.3.	Intégré dans le récepteur ou fonctionnellement séparé, au choix du fournisseur du service.	Entièrement contenu dans le module de sécurité. Accepte des données série en provenance du décodeur de paquets et fournit à l'utilisateur des données série désembrouillées.	Incorporé au récepteur et comportant un lecteur de cartes à mémoire.	Fonctionnellement séparé des autres parties du récepteur au moyen d'une interface qui reste à normaliser.
Module de sécurité § 7	Carte à mémoire avec interface proposée pour normalisation à l'ISO [ISO, 1986].	Module intégré ou amovible ou carte à mémoire.	Unité à microprocesseur contenant un logiciel d'application pour exécuter tous les algorithmes de déchiffrement et le traitement des protocoles de données.	Carte à mémoire avec interface proposée pour normalisation à l'ISO.	Deux solutions proposées: – la carte à mémoire ou – un module incorporé.

RÉFÉRENCES BIBLIOGRAPHIQUES

ISO [1986] TC/97/SC17/WG4/N97 Integrated circuit card with contacts, part III. Electronic signals and exchange protocols.

Documents du CCIR

[1982-86]: 11/422 (Rev.1) (Spécification des systèmes de télétexte, Projet de brochure descriptive du CCIR).
[1986-90]: a. GTIM 10-11/3-116 (France); b. GTIM 10-11/3-117 (Royaume-Uni).

BIBLIOGRAPHIE

BECKER, H. et PIPER, F. *Cypher Systems. The Protection of Communications.* Northwood Books – ISBN 719825717.

BRADSHAW, D.J., et WRIGHT, D.T., [16-17 septembre 1986] BBC Datacast - Conditional Access Operation, IERE Pub. No. 69, 99-105. Londres, Royaume-Uni.

DENNING, D. *Cryptography and Data Security.* Addison Wesley. ISBN 0-201-101-50-5.

GUILLOU, L. [novembre 1980] Radiodiffusion à péage pour application au télétexte Antiope. Congrès international sur les systèmes et services nouveaux de télécommunications, Liège, Belgique.

GUILLOU, L. [avril 1984] Smart card and conditional access. Eurocrypt 1984, La Sorbonne, Paris, France.

ISO [1987] TC97/SC17/WG4. Identification cards. Integrated circuits with contact. ISO Dis 7816.

MASON, A. G. [1985] A pay-per-view over-air addressing system specified for direct broadcasting by satellite. IERE Publication No. 62.

WRIGHT, D.T., et EDWARSON, S.M., [27 - 28 octobre 1986] Key Management in Broadcast Conditional Access Systems. IEE Conf. Pub. 269, 104-109. Londres, Royaume-Uni.

Documents du CCIR

[1982-86]: 11/139 (UER); 11/307 (France); 11/308 (France); 11/379 (Canada).

[1986-90] 11/35 (Royaume-Uni); 11/36 (Royaume-Uni); 11/40 (Royaume-Uni); 11/122 (France).

ANNEXE I

TERMES ET DÉFINITIONS LIÉS AUX SYSTÈMES DE RADIODIFFUSION A ACCÈS CONDITIONNEL

Embrouillage [en radiodiffusion] (scrambling, aleatorización)

Altération des caractéristiques d'un signal image/son/données radiodiffusé pour empêcher la réception non autorisée de l'information en clair. Cette altération est un processus bien défini, commandé par le système à accès conditionnel (côté émission).

Désembrouillage [en radiodiffusion] (descrambling, desaleatorización)

Restauration des caractéristiques d'un signal image/son/données radiodiffusé pour permettre la réception de l'information en clair. Cette restauration est un processus bien défini, commandé par le système à accès conditionnel (côté réception).

Note 1. – Les termes «embrouillage» et «désembrouillage» s'appliquent aussi bien aux signaux analogiques qu'aux signaux numériques.

Note 2. – Ces termes ne doivent pas être utilisés pour désigner des processus tels que la dispersion d'énergie dans un système à satellites.

Commande de l'accès conditionnel

La fonction de la commande d'accès conditionnel à l'émission est de produire les signaux de commande d'embrouillage et les «clés» correspondant au service.

La fonction de la commande d'accès conditionnel à la réception est de produire les signaux de commande de désembrouillage en même temps que les clés correspondant au service.

Note. – Le mot «clé» est utilisé dans les définitions précédentes avec un sens général équivalent à celui qui est utilisé dans la Question 37/11.

Les termes «chiffrement» et «déchiffrement» s'appliquent à des méthodes utilisées pour protéger et interpréter certaines des informations contenues dans les messages relatifs à l'accès qui doivent être diffusés de l'extrémité émettrice à l'extrémité réceptrice des fonctions de commande d'accès conditionnel.

BIBLIOGRAPHIE

Documents du CCIR

[1982-86]: 11/139 (UER); 11/228 (Groupe de travail Terminologie).

ANNEXE II

SYSTEMES DE RADIODIFFUSION A ACCES CONDITIONNEL: EXEMPLES DE PRINCIPES DES SYSTEMES DE CHIFFREMENT A CLE PARTAGEE POUR LES SERVICES DE RADIODIFFUSION DIRECTE PAR SATELLITE, Y COMPRIS LE TELETEXTE

1. Description du système à accès conditionnel utilisant l'adressage sur antenne employé au Royaume-Uni

1.1 Systèmes à accès conditionnel avec adressage sur antenne

La Figure 3 illustre les fonctions de base d'un système de chiffrement pour la télévision directe par satellite, avec adressage sur antenne. Un mot de contrôle (CW), qui change par exemple toutes les 10 secondes, sert à commander l'embrouillage du signal de télévision A. On obtient ainsi le signal embrouillé CW(A). Le mot de contrôle est transmis au récepteur après avoir été chiffré à l'aide de la clé supplémentaire S. Ce cryptogramme, qui contient aussi des données se rapportant au programme, par exemple le prix, est transmis dans un paquet de message de contrôle de titre d'accès ECM [UER, 1986]. La clé supplémentaire S est commune à tous les abonnés mais, contrairement au mot de contrôle, elle change peu fréquemment, par exemple une fois par mois. Grâce à ces longs intervalles entre les changements de la clé S, celle-ci peut être transmise à chaque abonné par le processus d'adressage sur antenne. La clé S ainsi que les messages de titre d'accès des abonnés (M) sont chiffrés à l'aide de la clé de distribution, D, de chaque abonné. Ces cryptogrammes sont envoyés dans des paquets EMM, adressés individuellement à des récepteurs séparés. Mason [1986] donne une description complète du système.

1.2 Réduction de la durée du cycle de validation - le cryptogramme partagé

La Figure 4 représente le format d'un cryptogramme partagé, qui permet de réduire le nombre total de bits à transmettre pendant le cycle de validation de l'abonné. Le cryptogramme de la Figure 4 englobe 23 abonnés, qui représentent un groupe d'abonnés. Tous les membres du groupe se partagent la même adresse principale, qui est utilisée pour l'accès au cryptogramme, et la même clé de distribution, qui sert à déverrouiller le cryptogramme. Etant donné que chaque membre du groupe a besoin de la clé supplémentaire à 56 bits pour récupérer le signal de télévision, l'excédent en bits est réparti entre les 23 abonnés. Il en va de même pour le mot de mode de 4 bits et pour l'adresse principale de 24 bits. L'ensemble des 84 bits est transmis au groupe tout entier plutôt qu'à chaque abonné individuellement. Ainsi, pour un groupe de 23 membres, il suffit de transmettre 3,65 bits par abonné. Ce budget permet d'obtenir un mot d'abonné de 12 bits qui peut assurer 12 services d'abonnement de base indépendants, 6 services superposés indépendants, ou des jetons pour taxation à la consommation. Ces derniers peuvent être utilisés pour des services quelconques, à condition d'être tous gérés par un exploitant de service commun. Le mot de mode identifie l'option qui est en cours de transmission. On peut utiliser un plus petit nombre de bits pour le mot d'abonné: par exemple, un système d'abonnement à un service de base unique nécessiterait un seul bit. Cela permet de réduire dans des proportions beaucoup plus grandes la durée du cycle de validation de l'abonné: par exemple, l'emploi d'un mot d'abonné de 12 bits divise normalement par 6,5 la durée de ce cycle, alors qu'un mot d'abonné de 1 bit la divise par 20.

1.2.1 Stratégie pour éliminer les clés de distribution volées

S'il est reconnu qu'un abonné est devenu un pirate, cette clé doit être supprimée. Il faut appliquer une méthode pour éviter de neutraliser d'autres abonnés qui utilisent la même clé en partage.

On obtient ce résultat en mettant en mémoire dans le dispositif de sécurité du récepteur, non pas une mais deux clés secrètes. La première clé est la clé de distribution partagée et la seconde est la clé unique (U); cette dernière n'est pas partagée, elle est différente pour chaque abonné. Lorsqu'un pirate est repéré, une nouvelle clé de distribution partagée (D_{new}) est envoyée individuellement à chacun des autres abonnés, qui sont de bonne foi; pour cela, on procède à un chiffrement de D_{new} au moyen de la clé unique (U) de ces abonnés; voir la Figure 5. Prenons un exemple: X, Y et Z sont les abonnés faisant partie d'un groupe donné qui utilise en partage la clé de distribution (D_{old}) et X est repéré comme pirate. On envoie la clé (D_{new}) aux abonnés Y et Z, en émettant $UY(D_{new})$ et $UZ(D_{new})$. Il est clair que le format pour la transmission de U(D) est beaucoup moins efficace que la clé partagée, mais cela n'a aucune importance, parce qu'on n'a affaire qu'à un petit nombre d'abonnés. Un radiodiffuseur peut être certain que les abonnés de bonne foi ont reçu la nouvelle clé de distribution (D), en émettant U(D) jusqu'à ce que les abonnés aient fait parvenir deux redevances d'abonnement. Comme la durée du cycle est probablement inférieure à une minute, le radiodiffuseur peut avoir la certitude que la nouvelle clé a été reçue. Cette certitude repose sur l'hypothèse que chaque abonné du groupe regarde les programmes pendant plus d'une minute au cours d'une période d'abonnement qu'il a achetée.

1.3 Transmission du crédit et du prix du programme sur antenne pour la taxation à la consommation

Il faut assurer une grande sécurité pour la transmission du crédit sur antenne, dans le cas d'un service complet avec taxation à la consommation. On y parvient avec certitude si les principes adéquats sont respectés.

1.3.1 Information de crédit sur antenne

La valeur d'une somme d'argent ne peut pas être envoyée sur antenne avec un chiffrement par une clé K, sous la forme K(MONEY). Cela est très hasardeux parce que le message MONEY n'est pas unique. Supposons que MONEY soit un code transmis qui représente une somme d'argent croissant de façon monotone, et que la transmission de la valeur "tout en zéros" pour le code représente un crédit nul pour un abonné. Le chiffrement de ce code avec la clé K donne une certaine séquence de bits pour K(MONEY). Un pirate peut ajouter de l'argent au crédit stocké dans le récepteur, sans connaître la clé K, simplement en modifiant la séquence de bits de K(MONEY). Quand le récepteur déchiffre ce nouveau message au moyen de la clé secrète K, le texte en clair doit être différent de zéro. La raison en est qu'il ne peut y avoir qu'une seule application du texte chiffré sur le texte en clair. Etant donné que le texte chiffré initial signifiait "crédit nul", toute modification doit donner la signification "crédit non nul". Le pirate peut donc ajouter du crédit, mais il ignore le montant.

On résout ce problème en ajoutant à la valeur de la somme d'argent une clé qui, si elle n'est pas reconnue, ne sera pas acceptée par le récepteur. A cet effet, on envoie le signal D(M,S), où D est la clé de distribution et S la clé supplémentaire. Pour pouvoir valider les bits de "money" (M) au moyen de la clé S, le récepteur doit être certain que la clé supplémentaire S a été correctement reçue. Pour ce faire, on émet le signal S(P,CW,S); voir le § 1.3.4.

1.3.2 Transmission de jetons de sommes d'argent

Le cycle de validation étant répétitif, il faut appliquer pour la transmission des jetons une méthode qui permette au récepteur d'accepter un nouveau paiement, mais qui l'empêche d'accumuler continuellement le même paiement à chaque répétition du cycle. Par ailleurs, il faut faire en sorte que les répétitions locales d'un ancien texte chiffré ne "trompent" pas le dispositif de sécurité du récepteur et ne le conduisent pas à accepter des paiements antérieurs plus d'une fois. Comme le canal de radiodiffusion permet seulement la communication unidirectionnelle, ces conditions doivent être remplies lorsque la cadence des paiements n'est pas synchrone avec la cadence de réception des paiements par le dispositif de sécurité.

La seule méthode que l'on connaisse pour satisfaire à ces critères fondamentaux consiste à transmettre sur le signal (M_T) le montant total de tous les paiements effectués au radiodiffuseur. Le dispositif de sécurité enregistre séparément dans ses mémoires "paiement" le total de tous les paiements qu'il a reçus (M_R) et la valeur du paiement (M_P). M_P est la différence entre M_T et M_R:

paiement effectué: $M_P = M_T - M_R$ pour $M_P > 0$.

De cette façon, il est impossible de "rater" des paiements; par ailleurs, les répétitions de paiements antérieurs n'entraîneront pas une augmentation de M_P: en effet, chaque fois qu'un paiement est accepté, M_R est mis sur la valeur reçue, M_T. Cela revient à dire qu'un paiement n'est accepté que si $M_T - M_R > 0$. Si l'on veut avoir un cycle de courte durée, il faut imposer une limite au nombre de bits utilisés pour transmettre la valeur M_T. La spécification du système MAC/paquets [UER, 1986] prévoit l'utilisation de 12 bits pour M_T, avec un maximum de 4 096 jetons.

1.3.3 Prix du programme

Les données relatives au programme (D) peuvent représenter le prix d'un programme. On peut utiliser la méthode suivante pour indiquer le prix: diminuer, toutes les 10 secondes, le montant enregistré dans la mémoire "paiements", au fur et à mesure que le programme est reçu. Une autre méthode consiste à demander un paiement unique au début du programme pour son acquisition totale. Si l'on opte pour cette deuxième méthode, on mettra en mémoire un numéro d'identification au moment où le programme est acheté, afin d'éviter un double achat; cela est nécessaire, par exemple, dans le cas où le récepteur est coupé pendant la transmission du programme.

Les données relatives au programme (P) sont "signées" (ce qui prouve qu'elles sont exactes) par la clé supplémentaire (S), de la même manière que les bits "money" de l'abonné. Pour obtenir cette "signature", on introduit la clé S dans le texte en clair du signal S(P,CW,S). Pour vérifier les données relatives au programme (prix) et les messages d'abonné (paiements), il suffit que le récepteur vérifie que la clé S a été reçue correctement; voir le § 1.3.4.

1.3.4 Connaissance de la bonne clé supplémentaire

Le contrôle de sécurité sur la clé supplémentaire (S) se fait à l'aide du signal S(P,CW,S). La propriété de ce signal est que la clé S est contenue dans le texte en clair et que, en même temps, elle est utilisée pour chiffrer ce texte. En déchiffrant le signal de validation D(M,S), le contrôle de sécurité dans le récepteur obtient tout d'abord la clé qui semble être la bonne clé supplémentaire S. Ensuite, il utilise cette clé S reçue pour déchiffrer le signal S(P,CW,S). Dans la mesure où le dispositif de sécurité est capable de déchiffrer le signal S(P,CW,S) et d'obtenir, dans le texte en clair, la même valeur pour la clé supplémentaire S, on a la quasi certitude que ce dispositif a reçu la bonne clé supplémentaire S.

La probabilité pour que le dispositif de sécurité donne une information erronée est approximativement de 2^{-n}, où n est le nombre des bits utilisés pour la clé S. Dans le système de l'UER [1986], on utilise 56 bits pour cette clé, ce qui donne 10^{-17} pour la probabilité de fausse détection.

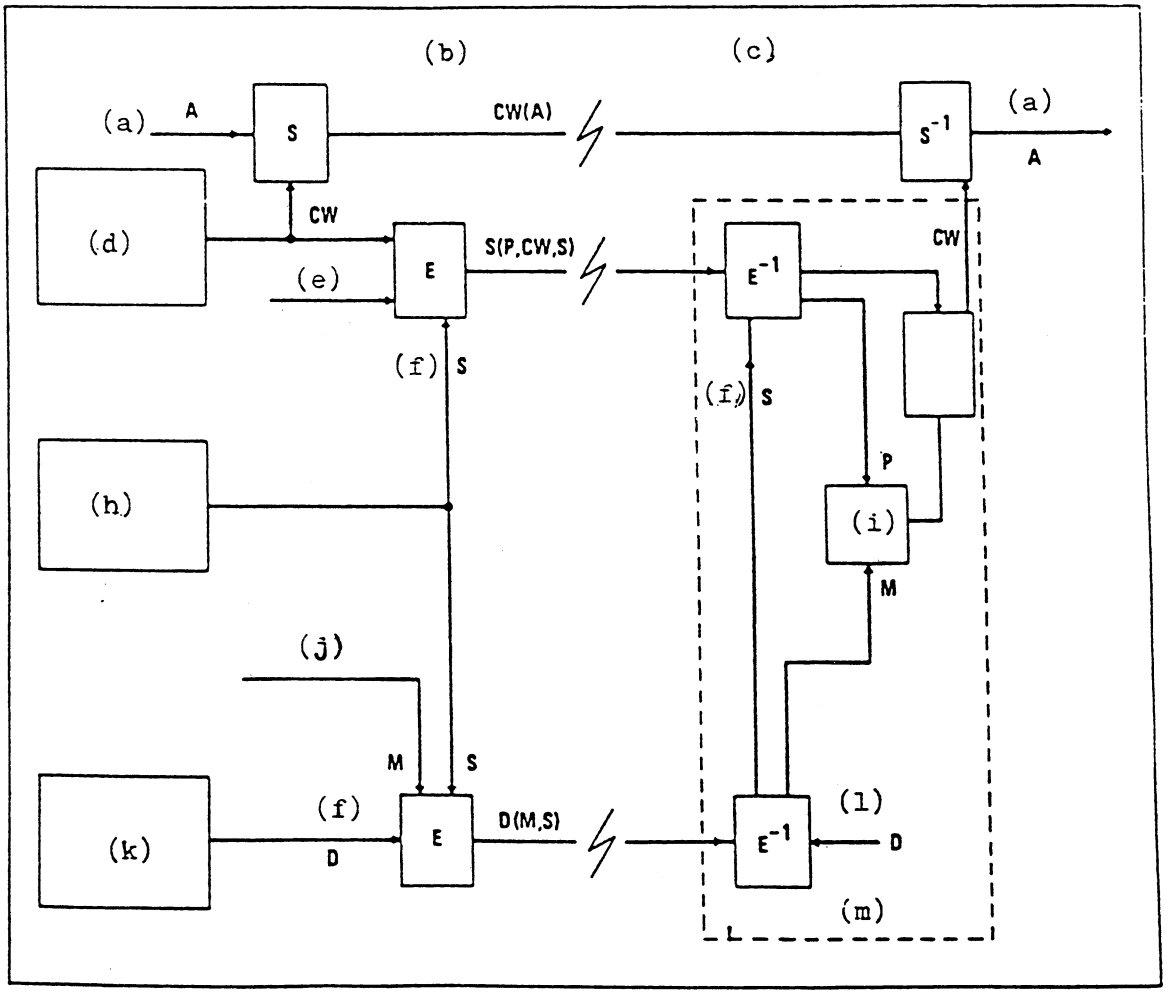


FIGURE 3 - Système de chiffrement de base

(a) signal de télévision
(b) émetteur
(c) récepteur
(d) mot de contrôle CW, changé toutes les 10 secondes
(e) données de programme, P
(f) clé
(g) porte
(h) clé supplémentaire, S, changée par exemple chaque mois
(i) mémoire
(j) message de client
(k) clé de distribution du client, D
(l) clé secrète du client
(m) dispositifs de sécurité

ARCHIVES U.I.T. GENEV

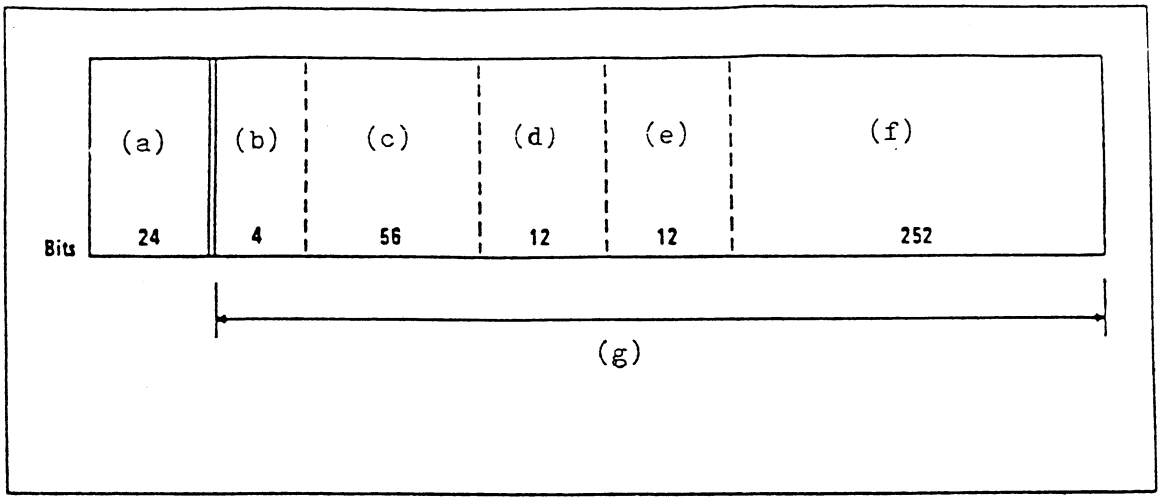


FIGURE 4 - Bloc de validation partagé

(a) adresse partagée

(b) mode

(c) clé supplémentaire, S

(d) client 1

(e) client 2

(f) clients 2 à 23

(g) bloc partagé, chiffré au moyen de la clé de distribution partagée, D

Note - Protection contre les erreurs (non représentée): trente (24, 12) mots de code de Golay.

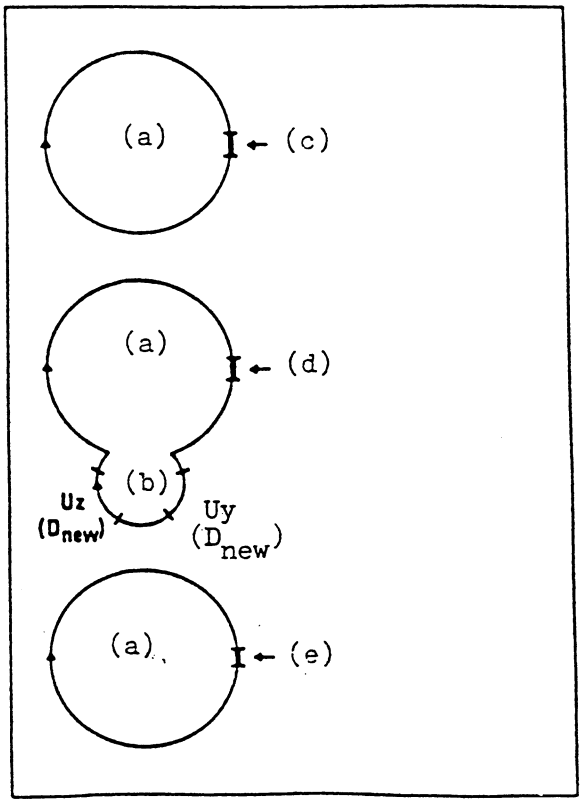


FIGURE 5 - Remplacement de la clé partagée D

(a) cycle D

(b) cycle U

(c) D_{old}: les clients X,Y,Z se partagent la clé D_{old}
(X,Y,Z)

(d) D_{new}: X devient un pirate et est éliminé
(Y,Z)

(e) D_{new}: le radiodiffuseur est sûr que Y et Z ont reçu D_{new}, parce qu'ils
(Y,Z) ont, l'un et l'autre, envoyé deux redevances d'abonnement.

2 - Description d'un système d'accès conditionnel utilisant l'adressage sur antenne système Eurocrypt

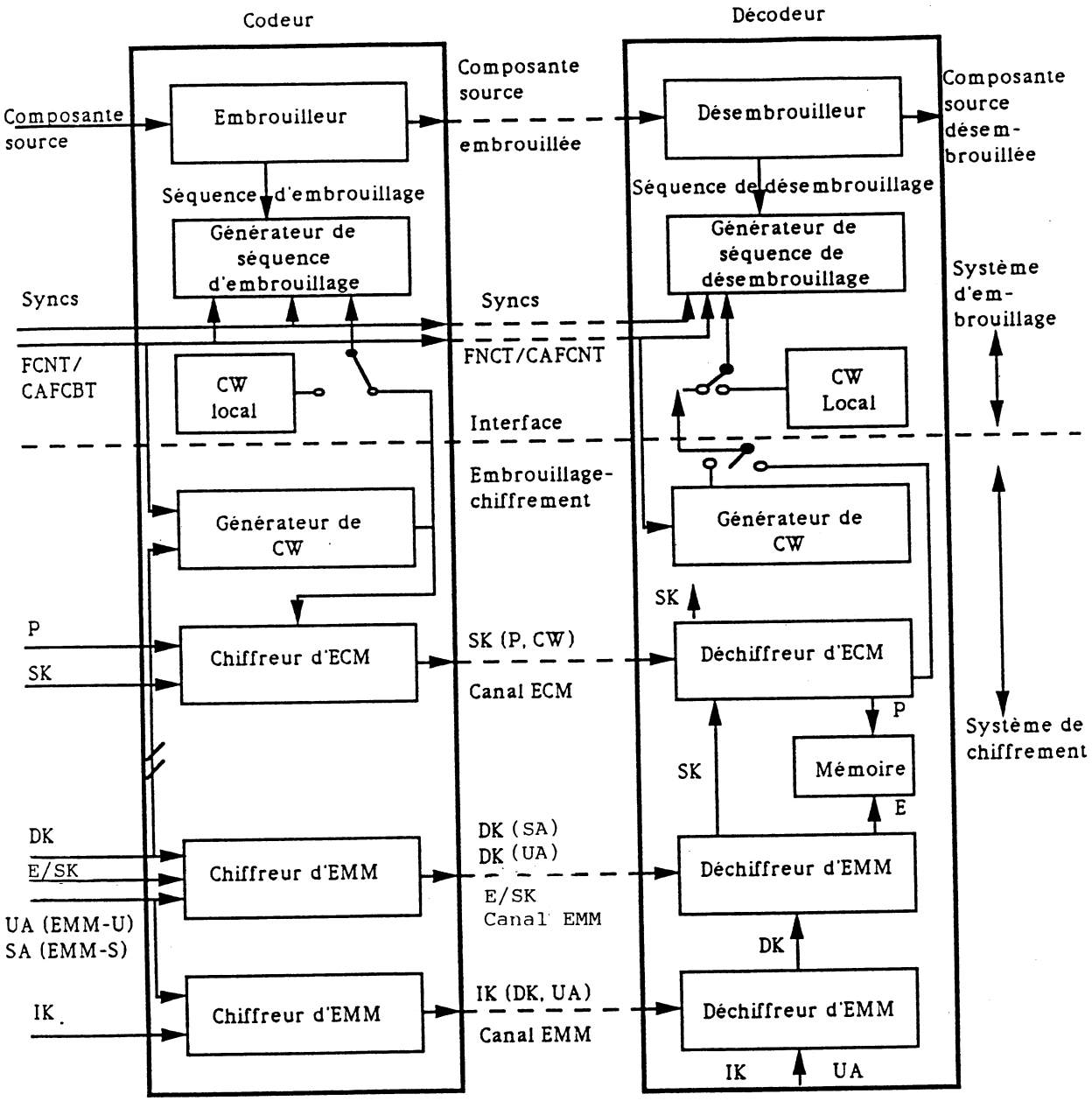
2.1 - Les systèmes d'embrouillage et de chiffrement

En référence à la figure 6, un mot de contrôle (CW) est utilisé pour initialiser le générateur de séquence d'embrouillage/désembrouillage.

Le mot de contrôle est émis, chiffré par la clé d'exploitation, dans les messages de contrôle des titres d'accès (ECM). Des données relatives au mode d'accès conditionnel du programme sont aussi présentes dans l'ECM. Le contenu des ECM est protégé contre la falsification par une procédure de signature. La clé d'exploitation (SK) est une information secrète contenue dans un processeur de sécurité. Si le processeur de sécurité reconnaît que les paramètres d'autorisation (titres d'accès) du récepteur s'accordent avec les paramètres d'accès conditionnel du programme, la clé d'exploitation peut être utilisée pour déchiffrer le mot de contrôle.

La clé d'exploitation est commune à tous les usagers. Les titres d'accès sont mis à jour périodiquement (par exemple chaque mois) ; la clé d'exploitation peut être modifiée dans des circonstances exceptionnelles. Aussi bien les titres d'accès que les clés d'exploitation peuvent être transmis aux usagers, en utilisant les techniques d'adressage sur antenne, dans des messages de gestion des titres d'accès (EMM). Les clés d'exploitation sont transmises chiffrées par une clé de distribution spécifique du fournisseur de programme. Le contenu des EMM est (de la même manière que pour les ECM) protégé par l'utilisation d'une procédure de signature. La clé de distribution peut être spécifique de chaque usager d'un groupe d'utilisateurs (voire de toute l'audience). Si la clé de distribution est spécifique de l'usager, elle ne peut servir qu'à envoyer des titres d'accès ou des clés à un usager unique repéré par son adresse individuelle (UA) dans un EMM individuel (EMM-U). Si la clé de distribution est commune à un groupe d'usagers, elle est utilisée pour envoyer des titres d'accès à un groupe d'usagers en utilisant un EMM partagé commun (appelé EMM-S). Dans la mesure où ceci permet une réduction du débit d'émission des EMM, cette technique est utilisée de préférence à la première. La première méthode serait mieux adaptée aux rares cas où un changement de la clé de distribution partagée est nécessaire.

La première clé de distribution d'un fournisseur de programme est également envoyée dans un EMM, chiffrée par la clé émetteur IK. Cette clé a la plus haute priorité dans le système de clé et est la seule capable d'ouvrir l'accès au processeur de sécurité à un nouveau fournisseur de programme. La clé émetteur est spécifique à chaque usager et est utilisée dans les EMM-U.



EMM : Message de gestion des titres d'accès
CW : Mot de contrôle
SK : Clé de service (ou clé d'exploitation)
FNCT : Compteur de trames (issu de la ligne 625)
CAFCNT : Comptage de trames pour accès conditionnel (issu de la ligne 625)
E : Titre d'accès du client
IK : Clé émetteur
UA : Adresse unique du récepteur
P : Donnée de programme
SK (P;CW) : P et CW chiffrés avec SK
DK (E;S) : E et S chiffrés avec DK
IK (DK, UA) : DK chiffré avec IK
DK : Clé de distribution
SA : Adresse partagée de récepteur

Figure 6 : Bloc diagramme général montrant la hiérarchie des clés d'un système d'accès conditionnel

2.2 - Hiérarchie et mise à jour des clés

L'utilisation fonctionnelle des différentes clés est illustrée sur la figure 7:

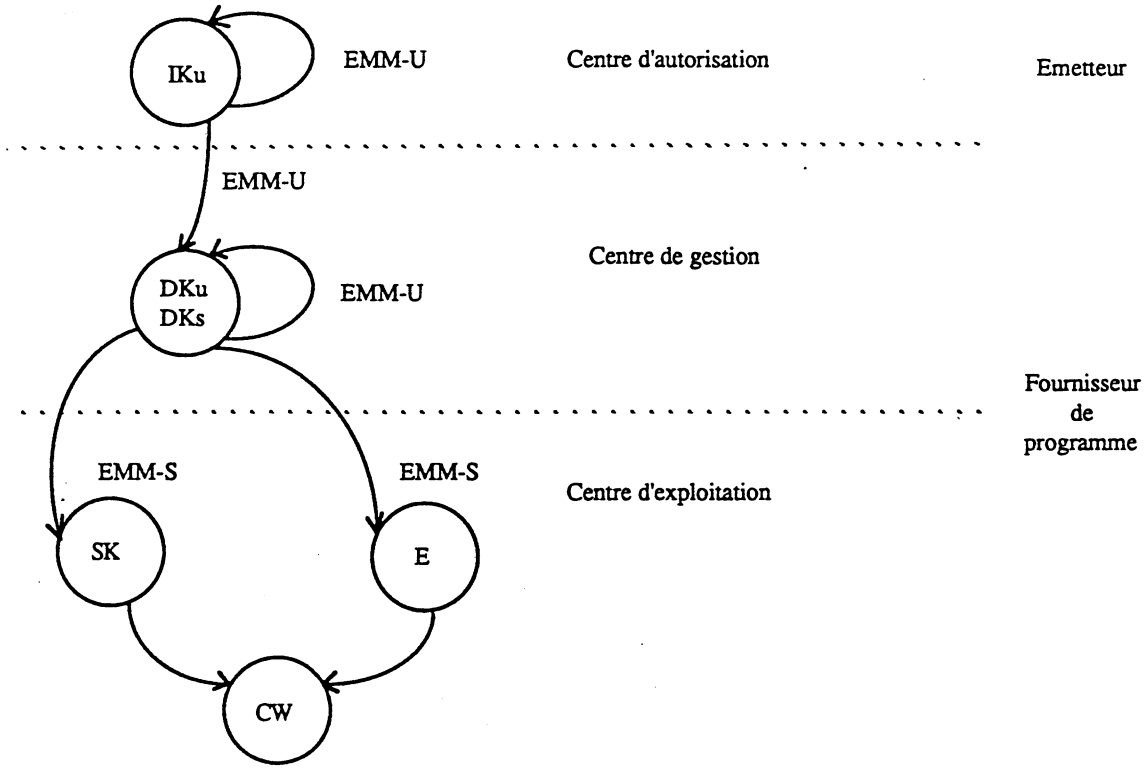


Figure 7 : hiérarchie des clés

2.2.1 - Clé émetteur

La clé émetteur introduit et met à jour tout type de clé secrète (DKu, DKs, SK, IKu).

La clé émetteur est la seule capable d'ouvrir l'accès pour un nouveau fournisseur de programme dans le processeur de sécurité en chargeant la première clé de distribution.

La clé émetteur est utilisée seulement dans des messages individuels (EMM-U).

2.2.2 - Clé de distribution

La clé de distribution unique DKu peut mettre à jour les DKs du service via les EMM-U.

Les clés de distribution partagées introduisent ou mettent à jour les clés d'exploitation et des titres d'accès via des EMM-S ; DKu peut aussi être utilisée pour cela avec un EMM-U mais l'intérêt en est moindre du fait de l'accroissement du débit de données.

2.2.3 - Clé d'exploitation

SK est utilisée pour signer un ECM et pour chiffrer un mot de contrôle.

2.2.4 - Organisation de la hiérarchie des clés

On peut envisager 2 scenarii principaux :

- le centre d'autorisation est en charge de la gestion des clés secrètes (introduction et mise à jour) :

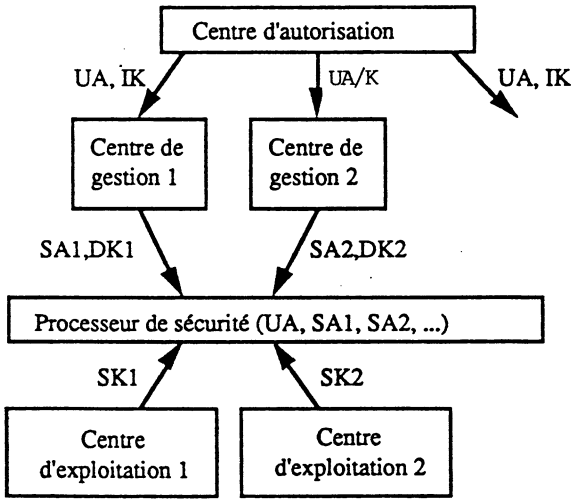
. l'émetteur introduit et met à jour DK et SK avec IKu,

. le fournisseur de programme met à jour les titres d'accès E avec DKs ;

- le centre d'autorisation est en charge de l'initialisation du fournisseur de programme mais délègue ensuite la gestion des clés appartenant au service :

. l'émetteur introduit DKu (en utilisation IKu),
. le fournisseur de programme introduit et met à jour DKs, SK et E.

L'organigramme des opérations peut être représenté comme suit :



Introduction des clés de distribution

Introduction de la clé de session, mise à jour des titres d'accès (et rarement mise à jour des clés de distribution et d'exploitation)

Mise en mémoire des clés d'exploitation SK1, SK2, ... et des titres d'accès

Calcul de CW

2.3 - Sécurité du système

2.3.1 - Intégrité des ECM et EMM

Deux niveaux de données sont transmis dans les ECM et EMM :

- les données secrètes qui seront transmises sous forme chiffrée (CW, clés secrètes),

- les données non secrètes dont le contenu doit bénéficier d'un haut niveau de protection (paramètres d'accès conditionnel, titres d'accès, adresse unique ou partagée) et qui utilisent une procédure de signature.

Pour des raisons de règlementation nationale, il peut être nécessaire d'envoyer les titres d'accès de manière confidentielle. Dans ce cas, les titres d'accès sont embrouillés ; cette fonctionnalité est optionnelle.

La structure des messages est alors un texte clair, suivi le cas échéant, d'un champ embrouillé et terminé par un champ de signature qui signe la totalité du message.

Structure de l'EMM :

Adresse usager (UA, SA) titre d'accès	(clé secrète)	signature
Texte clair ou embrouillé *	Chiffré	Signature

(clé secrète) : optionnel

* le texte embrouillé est optionnel et ne vaut que pour la description des titres d'accès ; on peut choisir cette option pour des raisons de règlementation nationale.

Structure des ECM :

Paramètres d'accès conditionnel	Môt de contrôle	Signature
Texte clair	Chiffré	Signature

La modification de quelque champ que ce soit est rendue impossible à travers le contrôle de la signature.

2.3.2 - La sécurité à partir de la hiérarchie des clés

La sécurité du système est obtenue par l'introduction de deux niveaux différents de clés. Les clés uniques et les clés partagées. La possession de clés pour un service est la première condition pour y avoir accès ; la seconde condition est que les titres d'accès (abonnement, crédit de consommation) correspondent aux conditions d'accès du programme pour autoriser l'utilisation de la clé d'exploitation SK. Lorsqu'on supprime un abonné, il n'est pas nécessaire de changer les clés, il suffit de ne plus mettre à jour les titres d'accès. Il n'y a à utiliser les DKs pour mise à jour que lorsque les clés d'exploitation sont découvertes par des pirates. L'utilisation des clés uniques (IKu ou DKu) est exceptionnelle et réservée à la mise à jour des DKs. La mise à jour des DKs requiert plus de capacité parce qu'il est nécessaire d'émettre des EMM-U pour adresser individuellement tous les membres du groupe. Bien que le piratage d'une clé unique soit d'un moindre intérêt, puisqu'elle s'applique à un usager unique, une telle clé peut aussi être mise à jour.

2.3.3 Sécurité à travers le processeur de sécurité

Le processeur de sécurité doit fournir une capacité de mémorisation de données secrètes incluant un algorithme pour décoder les champs chiffrés et pour contrôler l'intégrité des données. Le système est suffisamment flexible pour permettre l'amélioration du processeur de sécurité en changeant l'algorithme, en accroissant la capacité de traitement (introduction de nouvelles conditions d'accès) ... sans nécessiter de changer les récepteurs. Cette fonctionnalité est plus aisément réalisable si le processeur de sécurité est sous forme enfichable (carte à mémoire ...). Le processeur de sécurité doit être conçu de manière à éviter tout autre usage du mécanisme de sécurité que ceux pour lesquels il a été réalisé.

2.3.4 - Sécurité de la transmission

L'intégrité de la transmission de tous les paramètres décrivant un titre d'accès (thème/niveau, dates, crédit, numéro de programme, ...) est assurée par la méthode de signature. Il est alors impossible de modifier avec succès un ou plusieurs bits du message parce que le contrôle échouerait.

Pour la transmission d'un crédit, on a retenu deux méthodes :

- transmission du montant total de crédit acquis pour un élément de programme. Ce montant total est mémorisé dans le processeur de sécurité. L'achat de tout nouveau programme n'est possible que si le crédit résiduel (montant total du crédit, montant total du coût) est supérieur ou égal au coût du programme. Le montant total est transmis avec une date d'accréditation ;

- transmission d'un supplément de crédit pour un élément de service ; ce supplément de crédit est ajouté au montant total dans la carte. Ce supplément de crédit est associé à une date d'accréditation de manière à s'assurer que le même crédit n'a pas été ajouté plusieurs fois dans le processeur de sécurité.

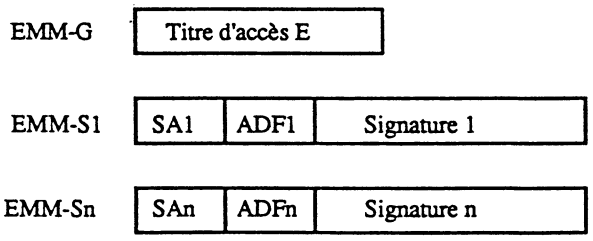
2.4 - Les messages partagés EMM-s

Le but des EMM-s est de réduire en conséquence le débit de données des messages de gestion. Les usagers du même groupe reçoivent la même mise à jour de leurs titres d'accès.

En supposant qu'un titre d'accès E doit être envoyé pour mettre à jour l'abonnement d'usagers, le message peut être :

- un EMM général (EMM-G), interprété par tous les récepteurs, pour décrire un titre d'accès commun.

- des EMM-s pour adresser des groupes d'usagers.



où :

E	est le titre d'accès à renouveler
SA1	est l'adresse partagée d'un groupe de 256 usagers
ADF1	est le champ d'adresse (256 bits) où un bit est affecté à chaque usager (si le bit est égal à 1, le titre d'accès est mis à jour, si le bit est égal à 0, le titre d'accès n'est pas mis à jour)
La signature	est la signature de E, SAi, ADFi en utilisant la clé de distribution DKi.

Cette méthode permet une réduction en conséquence du débit de données, 256 usagers partageant le même message (à comparer à un EMM-U où un message est utilisé pour chaque usager).

REFERENCES BIBLIOGRAPHIQUES

MASON, A., [septembre 1986] The principles of the over air addressed pay-per view encryption system for direct broadcasting by satellite and teletext. IERE Conf. Pub., No. 69.

UER [1986], Spécification des systèmes de la famille MAC/paquets, UER Tech.3258.

BIBLIOGRAPHIE

U.K. Department of Trade and Industry, London [1987] World system teletext and data broadcasting specification