CCETT

CENTRE COMMUN D'ETUDES DE TELEVISION
ET TELECOMMUNICATIONS

TSA/T/8/75

RENNES, le 11 Juin 1975

- DISCRET -

Rédacteur :

B. MARTI.

DOCUMENT DE DEFINITION

A - DEFINITION DU PROJET

1- Généralités

Le projet a pour but l'étude d'un système pour le cryptage et le décryptage d'émissions de télévision, la réalisation d'une source de signal crypté et d'une cinquantaine de terminaux expérimentaux de première génération. La date prévue pour la fin de cette étape est le mois de Janvier 1976. Le système de cryptage doit rendre difficile, sinon pénible la lecture d'une image télévisuelle et empêche la reconnaissance de textes et de sigles commerciaux. La voie son normale de l'émétteur est utilisée pour avertir les téléspectateurs non abonnés du caractère particulier de l'émission. Le son destiné à l'émission cryptée est transmis par multiplexage aux signaux d'image, d'échantillon impulsifs. le système de décryptage associé doit, tout en restant simple et bon marché, permettre l'utilisation de plusieurs services et leur différenciation, l'abonné d'un service ne pouvant pas recevoir les émissions destinées à des services auxquels il n'est pas abonné.

2- Principe du brouillage

Une suite de nombres binaires, en séquence pseudo-aléatoire de longueur supérieure à 300 permet de déterminer un choix parmi des paramètres du signal vidéo transmis : le premier de ces paramètres est la polarité, le second la phase par rapport aux signaux de synchronisation. Cette séquence pseudo-aléatoire est initialisée à chaque trame à sa valeur initiale, qui constitue la clé de codage. Ainsi les lignes homologues de deux trames successives, qui représentent deux lignes adjacentes sur l'écran, sont associées au même mot binaire. On asservit la loi de polarité à la parité de la trame : ainsi ces deux lignes adjacentes sont de polarité inverse. Il se crée de la sorte une compensation statistique faisant apparaître un niveau de luminance sensiblement moyen, tendant à faire disparaître les détails et les contrastes de l'image même en l'absence de décalage par rapport aux signaux de synchronisation. Ceci s'assortit d'un fort papillotement à fréquence image. Le déchiquètement crée par le décalage complète le brouillage en faisant disparaître les structures verticales laissées intactes par le processus d'inversion.

3- Objectifs 1975

Compte tenu de l'objectif final relatif à la fourniture de 50 terminaux d'abonnés pour le début de l'année 1976, ce qui constitue l'objectif global du laboratoire, il a été résolu de se fixer les ojectifs intermédiaires suivants :

1ere étape : 1er Juillet 1975

A cette date, l'ensemble des options techniques du système devront avoir été déterminées. Le terminal d'abonné devra être défini y compris pour ce qui concerne les modifications à apporter aux récepteurs de télévision. Les consultations auprès des sous traitants éventuels (Codiaco, Cerme)

.../...

devront être commencées. Le 15 Juillet au plus tard, devront être connues les conditions de prix et de délais relatives à cette sous traitance.

2ème étape : 15 Décembre 1975

A cette date, les marchés de réalisation des terminaux devront être proches de l'étape de livraison des premières unités. La source de signal crypté devra avoir été réalisée et mise au point au laboratoire. Les procédures de réglage du terminal devront être déterminées.

3ème étape

Livraison et réception des terminaux : Elle devra commencer le 15 Décembre au plus tard et se terminer avant fin Janvier 76.

B- DESCRIPTION DU SYSTEME

Il est difficile de donner d'après l'état actuel des choses une description définitive du système. En effet certains essais doivent encore être menés pour vérifier la validité de certains des principes retenus. Les options possibles seront décrites à mesure.

1- Système de cryptage de l'image

Il se compose des éléments suivants :

- Générateur de séquence pseudoaléatoire
- Logique de synchronisation
- Inversion
- Ligne à retard (étage de décalage)
- La clé d'entrée.

1.1. Générateur de séquence pseudoaléatoire programmable

(Figure 1)

Ce générateur est un registre à décalage à 10 étages pourvu de 9 points de rebouclage dont le rebouclage direct entre le dernier et le premier étage. Les huit points intermédiaires sont mis en fonction uniquement si un état 1 est appliqué à l'entrée de commande de l'étage correspondant. Ainsi un mot de 8 eb définit la configuration exacte du générateur. Dans ces conditions, il existe (table de) n = 35 générateurs possibles ayant une longueur de séquence maximale (1 = 1023) et certainement un nombre voisin de 80 générateurs ayant une séquence de longueur voisine de 512. Ces longueurs étant supérieures au nombre de lignes que comporte une trame, les séquences ainsi définies couvrent la trame entière sans répétitions périodiques.

Ce générateur est chargé par une instruction résultant de la synchronisation de trame par une valeur initiale fixée par un mot de 10 eb. Le mot de configuration et le mot de synchronisation constituent la clé d'accès au système (Voir § 1.5).

L'étage de sortie de ce générateur fournit p éléments binaires destinés à la commande de l'étage de décalage et un élément binaire destiné à la commande de l'étage d'inversion. Soit α cet élément. Le signal transmis

.../...

est α pendant les trames impaires et $\bar{\alpha}$ pendant les trames paires. Etant donné que la séquence se répète identiquement à elle même à chaque trame, les lignes adjacentes se présenteront avec une polarité inverse l'une de l'autre.

1.2. Logique de synchronisation

Les impulsions de synchronisation du signal entrant sont détectées et sont utilisées pour commander un oscillateur à boucle à verrouillage de phase à 12 MHz d'horloge fournie par cet oscillateur sera utilisée par le système de ligne à retard. Elle servira aussi, à travers un système de comptage à refabriquer l'ensemble des signaux de synchronisation nécessaires : les suppressions de ligne et de trame, et les divers points caractéristiques de l'image utilisés notamment par le multiplex sonore et les signaux de contrôle du système d'inversion. La parité de la trame est détectée de manière à commander l'inversion α ,$\bar{\alpha}$.

1.3. Système d'inversion de polarité

Le signal vidéofréquence arrivant est transformé en un signal de vision. Ce signal de vision passe parallèlement sur deux amplificateurs de même caractéristiques générales à ceci près que l'un inverse et l'autre pas. Les deux signaux obtenus sont fournis à un système de commutation à deux entrées et une sortie, l'entrée de commande étant reliée à la sortie (α,$\bar{\alpha}$) du générateur de séquence pseudoaléatoire.

On introduit en outre, après la fin de la suppression ligne une impulsion de blanc d'environ 1 µs de durée destinée à servir de référence de "champ" au blanc des lignes inversées dans le récepteur et d'alignement CAG.

1.4. Système de décalage

Le système a été essayé avec une ligne à retard ayant un retard fixe de 2 µs. Le retard était donc codé avec un mot de 1 eb.
Il a été résolu d'essayer pour le prototype des lignes à retard programmables vidéo analogiques intégrés du type SAM 64. Ces lignes à retard sont formées de deux registres de 64 points. On entre les points sur une capacité ouverte par le registre d'entrée à partir d'un signal de départ d'entrée. Un signal de départ de sortie charge le registre de sortie qui commande la connection des capacités sur un bus de sortie et permet un retard entre le signal d'entrée et le signal de sortie dépendant du retard entre les signaux de départ d'entrée et de sortie. Ce retard peut être modifié au début de chaque ligne par programmation de compteurs. On peut utilisé pour cette programmation un mot de 6 eb au plus, ce qui conduit à utiliser la capacité totale de la ligne. La fréquence maximale d'utilisation étant de 12 MHz, le retard maximum sera de 5.33 µ. En fait, il ne semble pas souhaitable d'introduire de retard trop supérieur à 2 µs et l'utilisation de la moitié seulement de la capacité de la ligne (codage à 5 eb du retard) semble un compromis raisonnable Il n'y a pas intérêt à augmenter par trop ce retard car chaque ligne de l'image se trouve amputée d'une durée comprise entre I et 2 I selon le type de normalisation adoptée.

1.5. Clé d'entrée

Elle sera fixée sur la source par affichage d'un nombre de 18 eb. Dans la première partie du projet, la clé sera fixe. Dans une étape ultérieure dont les caractéristiques seront définies fin 75, la clé sera périodiquement

.../...

transmise par DIDON. L'émetteur sera donc composé d'un récepteur DIDON destiné à connaître le moment où la clé nouvelle sera transmise afin de conserver le synchronisme à l'ensemble du système.

On peut concevoir deux niveaux de service :

a) le service "bon marché" à clé fixe dont la période de variation sera mensuelle ou hebdomadaire, la clé matérialisée pouvant être périodiquement achetée ou fournie par abonnement. Le terminal correspondant est le terminal fourni à l'issue de la présente étape .

b) le service sophistiqué à clé variable avec une période de l'ordre de la minute.

L'abonné disposant du terminal adapté au service de type a)pourra accéder au service de type b)par acquisition du terminal DIDON en remplaçant le lecteur de la clé matérialisée par le branchement de la jonction de prise informatique. Le lecteur de clé du service a) aura une configuration extérieure compatible avec celle de la prise informatique.

2 - Système de cryptage du son

Le principe retenu consiste en la formation d'une impulsion modulée en durée par le son. La fréquence d'échantillonnage est de 15625 Hz ce qui limite la bande passante du canal à 7.5 kHZ environ.

3 hypothèses possibles encore en l'état actuel de l'étude pour le multiplexage de cette information avec l'information d'image.

a) Modulation en amplitude de la sous porteuse par l'impulsion à durée variable.

b) modulation en durée de la référence de blanc .

c) dérivation de l'impulsion à durée variable et mise en place d'une impulsion courte de 700 mv environ superposée au burst de sous porteuse et correspondant au front arrière, le front avant étant fourni par le signal de synchronisation. Une étude ultérieure permettra de déterminer un système compatible avec celui-ci et fournissant un signal de meilleure qualité.

L'idée actuellement envisagée consiste dans l'hypothèse 2-C à échantillonner le signal sonore à 2 fh soit 31250 Hz ce qui fournit 2 échantillons par ligne. On forme un échantillon x = A + B qui fournit l'impulsion définie plus haut. Cette impulsion d'amplitude comprise entre 400 et 700 mv est modulée entre ces limites en amplitude par y = A - B . Ce qui permettrait aux récepteurs simplifiés de démoduler A + B sous le forme d'un signal à 7,5 kHz et à ceux qui disposent d'un terminal plus élaboré de disposer d'un son à 15 kHz de bande passante.

3 - Terminal d'abonné

Le terminal d'abonné contient des éléments identiques à ceux du système de cryptage. On y retrouve :

- Le générateur de séquence pseudo-aléatoire
- l'horloge asservie et une partie de la logique de synchronisation
- Le système d'inversion de polarité
- La ligne à retard programmable
- Un dispositif de clé d'entrée

Cependant, la présentation de ce dernier diffère notablement de celle nécessitée par le cryptage. Il se compose d'une boîte extérieure munie d'une prise Amplenol 36 pts identique à celle utilisée pour le prise informatique. Danc cette boîte viendra s'enficher une clé, physiquement représentée par un morceau de circuit imprimé moulé portant sous le moulage les connections nécessaires à la fixation et la combinaison des 18 eb de la clé.

.../...

Seul diffère profondèment le dispositif de décryptage du son. Il se compose d'une bascule RS, mise à 1 par l'impulsion de synchronisation de ligne et remise à zéro par une impulsion détectée sur le signal. Le signal de sortie de cette bascule sert de signal d'entrée à un système de filtres comportant un passe bas dont la fréquence de coupure est de 7.5 kHz et un piège ("notch") réglé à 50 Hz. En effet, l'absence de signaux pendant la suppression trame crée un signal parasite à 50 Hz qu'il faut éliminé.

4 - Récepteur adapté

Afin de recevoir convenablement les émissions cryptées, les récepteurs actuels devront être modifiés. A cet effet le laboratoire acquerra un ou deux récepteurs grand public d'un modèle récent disposant déjà d'une prise magnétoscope. Cette prise permet la sortie du signal composite issu de l'étage F-I ou l'entrée d'un signal composite extérieur. Il faudra apporter toutes modifications nécessaires pour que le récepteur puisse à la fois fonctionner en sortie et en entrée d'un signal composite : le signal en sortie sera le signal crypté issu de l'antenne. Le signal à l'entrée sera le signal décrypté provenant du terminal.

En outre, la platine BF du récepteur devra utiliser non pas les signaux provenant de la sous porteuse du son mais les signaux insérés après leur décodage par le terminal DISCRET.

C - ECHEANCIER PREVISIONNEL

1 - A ce jour (20.04.75) ont été réalisés :

- maquette du crypteur image avec générateur de séquence , inversion et une unité de retard
- début de l'étude du crypteur son
- commande de 10 lignes à retard CCD Sam 64 (livraison prévue début mai)
- Etude d'éléments du récepteur (asservissement et synchronisatio

2 - Programme des mois de mai-juin

Réception et mise en oeuvre des SAM 64.
Réalisation du démodulateur BF.
Le choix définitif du mode d'insertion de la BF doit être fait avant le 10 juin.
Essais de l'inverseur vidéo du récepteur, choix du type de régulation de niveau de la voie inversée.
Etude des modifications à apporter au récepteur grand public (sortie vidéo, entrée vidéo au niveau composite).
Echéance de fin de juin : le schéma complet du récepteur et de ses annexes doit être obtenu et arrêté définitivement.

3 - Programme après juin

Début juillet : les consultations auprès des sous traitants doivent être terminées le 15 juillet, date de rigueur, et le marché passé dans la foulée.
Le début du dernier quadrimestre sera réservé à la mise au propre de la source et au suivi de la sous traitance.

.../...

Mise à jour du document au 2.06.75

A ce jour, fonctionnent le système de cryptage et le système de décryptage par inversion.
L'étude du système de retard à SAM 64 est commencé. Cependant face aux difficultés relatives à l'emploi de ce composant nouveau, il est envisagé d'utiliser des lignes conventionnelles de 2 X 1 µs (Sécré type YE 1029).
L'ensemble codage décodage à lignes conventionnelles doit fonctionner le 12 juin pour la visite de l'UER.

En ce qui concerne le son, les performances du système décrit au §2-C ont été vérifiées notamment en présence de bruit et semble donner satisfaction.