Le système de communication ultra-sécurisé SIGSALY à l'origine de notre monde numérique ?

Jon D. Paul

I. Motivation du projet SIGSALY

Après Pearl Harbor, le comité *US communications* déclara le développement d'un système de communication vocale totalement sécurisé comme une priorité de guerre de la plus haute importance. Le système SIGSALY était prêt en 1942, et fut déployé courant 1943.

II. La téléphonie secrète de Dudley

Homère Dudley chez *Bell Telephone Laboratories* (BTL) a abordé le problème du chiffrement de la voix en 1941, par la combinaison de son Vocoder avec une clé secrète aléatoire stockée sur des disques de phonographe. Une source de bruit aléatoire est échantillonnée pour produire la clé de chiffrement. La sortie de l'enregistrement clé est découpée en sous-bandes par une banque de filtres. Les sous-bandes sont échantillonnées en temps réel, quantifiées, combinées avec la sortie du VOCODER, et transmises via multiplexage temporel. Le processus de reconstruction nécessite une copie de l'enregistrement clé et un système de multiplexage synchronisé avec l'émetteur. Les sous-bandes déchiffrées et le signal de tonalité issus du VOCODER sont transmis à l'étage de synthèse pour reconstruire la voix.

III. Diagramme de blocs et concepts

Le brevet de Dudley sur la téléphonie secrète (Figure 1) décrit les concepts du VOCODER avec 6 niveaux de quantification sur les paramètres et un chiffrement de Vernam par addition modulo 6 des entrées et un masque jetable.

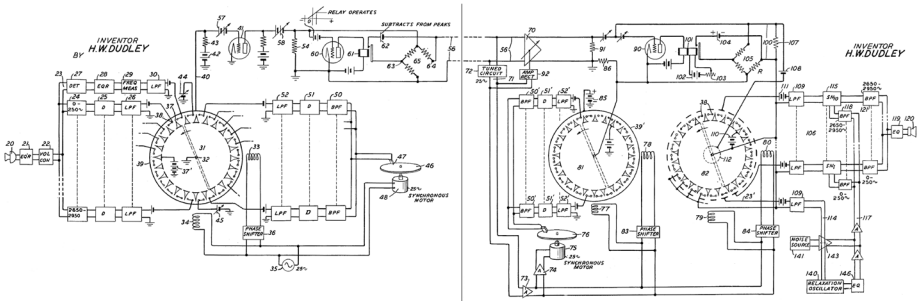

Figure 1 - Brevet US 3 985 958 (Chiffrement et Déchiffrement)

Les ingénieurs des BTL découvrirent que 6 niveaux de quantification étaient à peine suffisants pour les 10 sous-bandes du VOCODER dans SIGSALY. Le signal analogique était quantifié par des thyratrons 2050 (des tétrodes remplies d'argon) passants à 6

tensions différentes, par pas de 6 dB. Ce fut le premier exemple d'encodage non linéaire (compression) et le premier convertisseur analogique-numérique.

IV. Quantification de la tonalité par SIGSALY

Le canal de tonalité d'un VOCODER doit être quantifié avec une bien meilleure résolution que les 10 sous-bandes (Figure 2). Ce signal est d'abord quantifié sur 6 niveaux. Le signal résultant de cette quantification est soustrait du signal original, et la différence (le résidu) est amplifiée avec un facteur 6 puis elle-même quantifiée sur 6 niveaux.

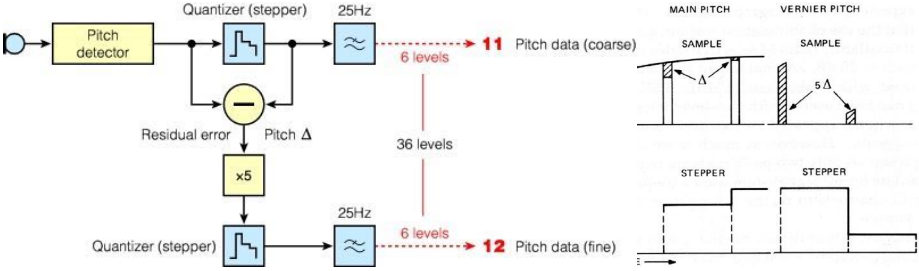

Figure 2 - La quantification de la tonalité de SIGSALY

Il s'agit donc d'une quantification en deux étapes: 6 niveaux à grosse maille, puis 6 niveaux à grain fin sur le signal résiduel. La combinaison des deux étapes permet de représenter la tonalité sur 36 niveaux (environ 5 bits), ce qui est une résolution suffisante pour obtenir une qualité de reconstruction acceptable. Cette technique de quantification largement utilisée aujourd'hui dans les convertisseurs A/D rapides pour vidéo, SDR, radar, ou tout autre processus de conversion à large bande.

V. Chiffrement de Vernam Modulo 6

SIGSALY transmettait les 12 paramètres du VOCODER sous la forme de signaux quantifiés sur 6 niveaux, qui représentaient les 10 sous-bandes de l'analyseur vocal, ainsi que les composantes à grosse maille et à grain fin du signal de tonalité. Le bruit blanc utilisé comme masque jetable était aussi quantifié sur 6 niveaux à une fréquence de 50 Hz. Comme les systèmes de transmission et de modulation étaient aussi basés sur cette échelle de 6 niveaux, l'addition s'effectuait modulo 6. Tout résultat d'addition dépassant 5 se voyait soustraire le niveau de tension équivalent au niveau 6 (Figure 3). La valeur d'origine pouvait être récupérée à la réception par l'opération inverse, équivalente à un « ou exclusif » (XOR).

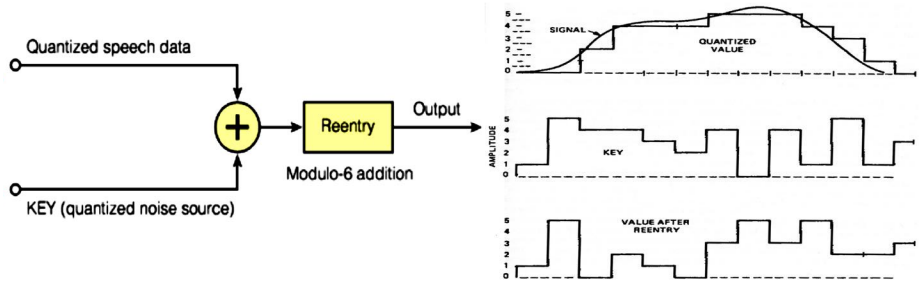

Figure 3 - Le chiffrement de Vernam modulo 6 de SIGSALY

VI. Résumé du processus de chiffrement SIGSALY

Le processus de chiffrement SIGSALY (Figure 4) commence par le découpage de la voix en 10 sous-bandes de 250 Hz par les filtres du VOCODER. Le VOCODER produit également un bit voix/non-voix ainsi qu'un signal de tonalité. Ces 12 paramètres traversent un filtre passe-bas pour réduire leur bande passante à 25 Hz. La voix ainsi compressée utilise 300 Hz de bande passante. Dans SIGSALY, les paramètres du VOCODER sont échantillonnés à 50 Hz et quantifiés sur 6 niveaux, sauf la tonalité qui nécessite 36 niveaux.

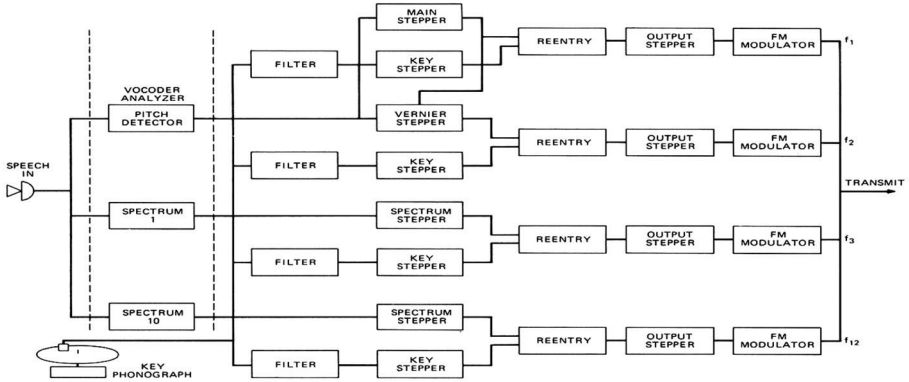

Figure 4 - Schéma de l'émetteur de SIGSALY (Chiffrement)

La clé de chiffrement est un bruit blanc. Ce bruit traverse une banque de filtres identique à celle du VOCODER. Chaque sortie est réduite à une bande passante de 25 Hz par des filtres passe-bas, échantillonnée à 50 Hz, puis quantifiée sur 6 niveaux comme les paramètres du VOCODER.

Les paramètres quantifiés sont ajoutés modulo 6 à la clé de chiffrement quantifiée. Il s'agit d'un processus équivalent au chiffrement de Vernam appliqué aux télétypes, une addition modulo 6 remplaçant le « ou exclusif » binaire. Le signal chiffré utilise une bande passante de 300 Hz.

Le processus d'étalement de spectre reçoit les 12 flux chiffrés et leur applique une modulation FM puis BLU (*Single Side Band*) avec 12 fréquences porteuses distinctes FDM (*Frequency Division Multiplexing*). Les 12 signaux sont additionnés pour créer un spectre étalé sur 3 kHz, qui est finalement transmis par radio en BLU. Le récepteur applique le processus inverse, en utilisant une clé identique et parfaitement synchronisée, pour récupérer les 12 paramètres du VOCODER. Ces paramètres entrent dans l'étage de synthèse du VOCODER et recréée la voix d'origine.

VII. Étalement de spectre dans SIGSALY

Les transmissions SIGSALY utilisaient des liens transocéaniques à ondes courtes, considérablement affaiblies (20 dB) par leur réflexion dans l'ionosphère.

SIGSALY utilisait une forme primitive d'étalement de spectre pour surmonter cet affaiblissement, grâce à la combinaison d'une modulation FM du signal principal et une modulation AM-BLU de chacun des 12 paramètres (Figure 5). Les 12 canaux étaient additionnés ensemble puis re-modulés en BLU avant transmission. Ceci étalait 12 canaux de 300 Hz 10 fois, soit une bande passante totale de 3 kHz.

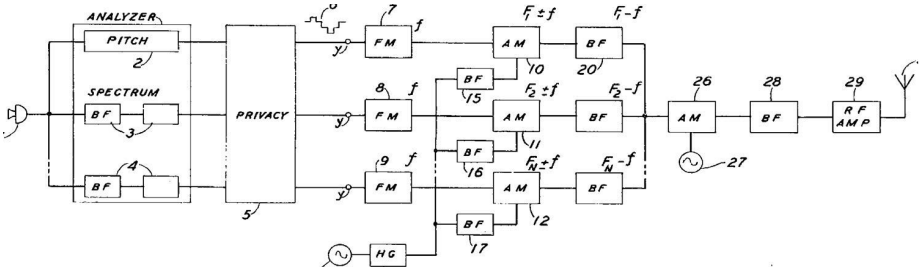

Figure 5 - Chiffrement et émetteur avec étalement de spectre de SIGSALY

L'utilisation de FDM (*Frequency Division Multiplexing*) par SIGSALY fut précurseur de toutes les techniques d'étalement de spectre. Des exemples plus récents incluent le CDMA et le GSM utilisés par les téléphones cellulaires, le Wi-Fi, la radio numérique terrestre ainsi que la télévision numérique terrestre (DVB-T) qui emploie la modulation COFDM (*Coded Orthogonal Frequency-Division Multiplexing*).

VIII. Construction et déploiement de SIGSALY

VIII.1. Caractéristiques et spécifications de SIGSALY

SIGSALY offre un chiffrement inviolable de la voix sur des liaisons radio téléphoniques transocéaniques. Le système fut en service de 1943 à 1946, période durant laquelle 12 terminaux furent en opération dans le monde. Le bureau du chiffre des puissances de l'Axe ne fut en mesure de déchiffrer aucune des 3000 audioconférences tenues via SIGSALY. Une machine SIGSALY avait des proportions gargantuesques (Figure 6), incluant 40 armoires, consommant 30 kW, pesant 3356 kg et occupant 232 m2 au sol.

Chaque terminal SIGSALY coûtait 1 million de dollars en 1943 (soit 15,5 millions de dollars en 2017). 13 techniciens étaient nécessaires pour opérer une seule machine en 24 heures sur 24 et 7 jours sur 7. Le refroidissement était un problème majeur, nécessitant une puissante climatisation. L'auteur a pu localiser le site de la machine SIGSALY installée à Paris, au 29 rue La Pérouse, près de l'Arc de Triomphe, dans un bunker des transmissions allemand abandonné (Figure 7).

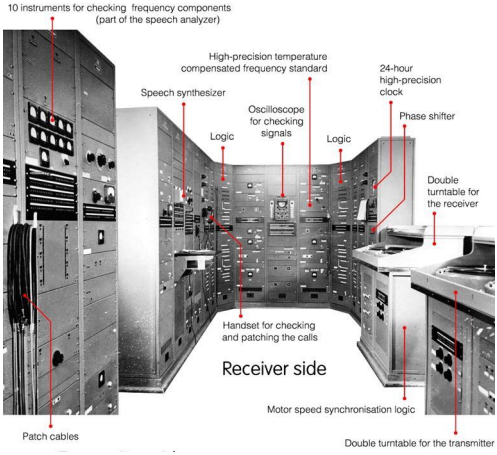

Figure 6 - Description des équipement d'un terminal SIGSALY

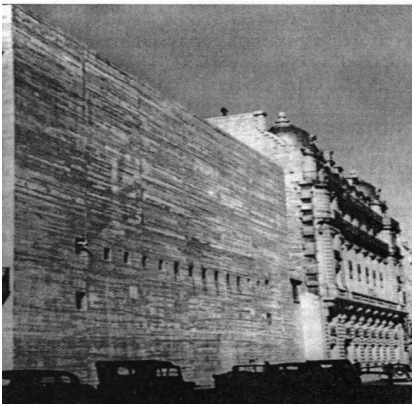

Figure 7 - SIGSALY dans Paris libéré, 1944, un bunker des transmissions allemand abandonné, US Army Signals Center, Europe

VIII.2. Masque jetable aléatoire sur phonogrammes, synchronisation

Selon le papier classifié de Shannon, un système de chiffrement inviolable nécessite une clé à usage unique de longueur égale à celle du message à transmettre.

SIGSALY utilisait 6 diodes à vapeur de mercure (10 cm x 40 cm) pour générer du bruit blanc. Les 6 canaux analogiques de sortie étaient quantifiés sur 6 niveaux de la même manière que les autres canaux du VOCODER. Comme le VOCODER avait 12 canaux chiffrés (10 sous-bandes et 2 canaux pour la tonalité, l'un à grosse maille et l'autre à grain fin) avec un taux d'échantillonnage de 50 Hz, SIGSALY nécessitait 600 clés aléatoires par seconde.

Le signal aléatoire quantifié sur 6 niveaux était modulé en FSK (*Frequency Shift Keying*) et enregistré sur des disques de 41 cm (nom de code SIGGRUV) avec un tourne-disque de précision (Figures 8 et 9). Chaque disque contenait 12 minutes d'aléa. Un disque maître n'était utilisé que pour deux impressions. L'un était conservé à Washington, D. C. dans les locaux de l'*Army Security Agency*. L'autre était envoyé à la machine SIGSALY distante par la valise diplomatique. Chaque paire de disques n'était utilisée qu'une seule fois.

Les clés d'émission et de réception étaient synchronisées avec précision. La synchronisation était affinée par les opérateurs jusqu'à une précision de 200 µs en ajustant manuellement la phase du signal temporel tout en écoutant la voix reconstruite, pour une meilleure intelligibilité.

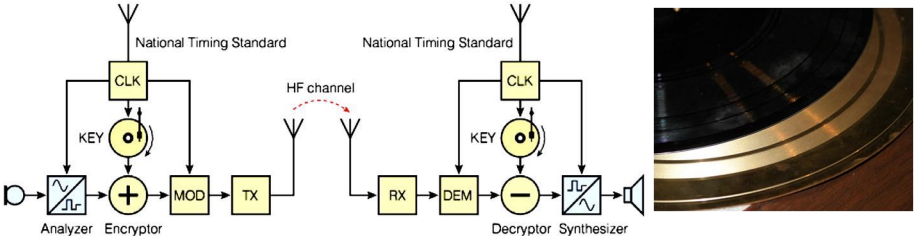

Figure 8 - Le synchronisation de la clé de SIGSALY et le disque SIGGRUV

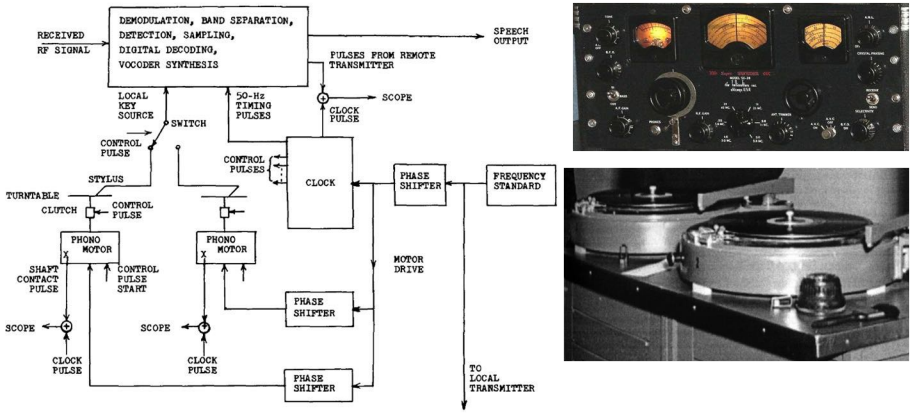

Figure 9 - Enregistrement de la clé de synchronisation, SX-28 SW Radio et tourne-disque 16"

VIII.3. Clients SIGSALY

Au total, 3000 audioconférences furent tenues via ce système durant la Seconde Guerre mondiale.

Le plus célèbre utilisateur de SIGSALY fut Winston Churchill, qui l'utilisa des centaines de fois, y compris pour organiser le débarquement de Normandie.

Le Général américain Leslie Groves (du Projet Manhattan), Hap Arnold *(US Army Air Forces*) et Chester Nimitz (*US Navy*) tinrent de nombreuses audioconférences avec SIGSALY.

Le Général Douglas McArthur (Figure 10) fit un usage intensif de SIGSALY pour diriger la campagne des Philippines (1944-1945) En 1946 et 1947, les 12 terminaux SIGSALY, ainsi que les pièces de rechange et la documentation, furent détruits par mesure de sécurité liée à la Guerre Froide.

Figure 10 - Le général Douglas MacArthur

VIII.4. Reconstitution de SIGSALY par le National Cryptographic Museum

La NSA (*National Security Agency*) et le NCM (*National Cryptographic Museum*) souhaitaient organiser une exposition SIGSALY, mais la NSA ne disposait d'aucun détail technique. Il ne s'agissait que d'une reconstitution extérieure sans aucune électronique.

VIII.5. Reconstruction de la Quantificateur par SIGSALY

SIGSALY implémenta la première quantification numérique et donc la première transmission PCM de la voix. Le Musée Crypto de l'auteur mena des recherches sur SIGSALY pendant 15 ans, et découvrit que le quantificateur à 6 niveaux de SIGSALY était le plus ancien convertisseur analogique-numérique connu.

L'auteur a conçu et construit une reconstitution du quantificateur de SIGSALY pour l'exposition du centenaire de Shannon. La reconstitution utilise les composants d'origine, comme les thyratrons 2050. Comme les terminaux SIGSALY et leurs plans furent détruits en 1946 pour des raisons de sécurité nationale, ce travail est basé sur les brevets SIGSALY, les informations de la NSA et les livres très détaillés du Lt. Donald Mehl, *805 U.S. Army Signal Corps*, qui était technicien et qui installait et entretenait les terminaux SIGSALY.

La Figure 11 représente le schéma du quantificateur. L'entrée analogique alimente une échelle logarithmique de résistances. Chaque barreau de l'échelle pilote la grille d'un thyratron 2050. Le niveau d'excitation du thyratron de 3,5 V est décalé à 1,0 V par une tension continue appliquée à la cathode. Les cinq thyratrons fonctionnent comme comparateurs avec un niveau de déclenchement à 1,0 V. Tandis que la tension d'entrée passe de 0 à 16 volts, les cinq thyratrons se déclenchent successivement et deviennent passants pour des valeurs d'entrée de 1, 2, 4, 8 et 16 volts. Ainsi la tension d'entrée est quantifiée (ou numérisée) selon chacun de ses six niveaux logarithmiques.

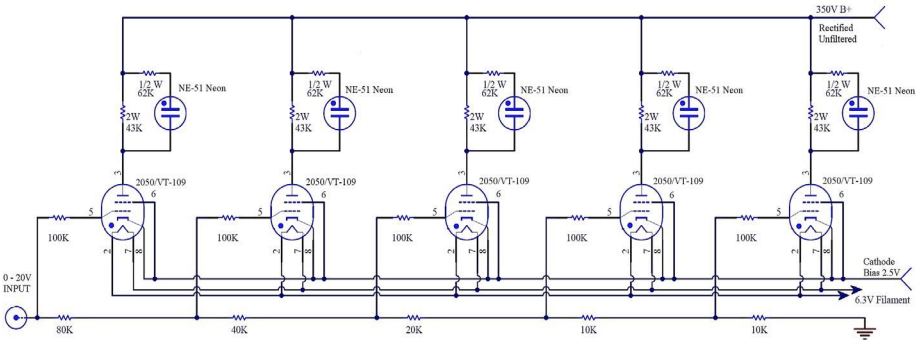

Figure 11 - Reconstruction du quantificateur de SIGSALY : schéma du premier convertisseur analogique-numérique

Le quantificateur reconstitué (Figure 12) dispose d'une base en polycarbonate transparent pour laisser apparaître le circuit. Un bouton-poussoir et un circuit RC permettent de générer un signal montant lentement de 0 V à 16 V. Un microphone externe peut également être branché pour montrer un niveau de quantification basé sur le volume sonore. La reconstitution intègre un préamplificateur de 100 dB dont la sortie est détectée pour fournir un signal à composante continue au quantificateur. Quelle que soit la source, l'entrée analogique est affichée sur un VU-mètre. La sortie quantifiée est représentée par des ampoules néon attachées à la résistance de plaque de chaque thyratron. Les cinq ampoules s'allument successivement tandis que chaque thyratron se déclenche, démontrant les six niveaux numérisés. La plaque B+ est alimentée par un courant alternatif rectifié mais non filtré.

Figure 12 - Reconstruction du quantificateur de SIGSALY

Selon la NSA, le NCM, et d'autres sources fiables, ceci est la toute première tentative de reconstitution d'une partie de SIGSALY. Ce quantifieur est disponible pour les musées et les conférences qui veulent en faire la démonstration.

IX. LES 11 INNOVATIONS DE SIGSALY

De nombreux ingénieurs des BTL travaillèrent longuement sur la conception de SIGSALY. Leurs efforts produisirent 32 brevets ; certains restèrent classifiés « secret » jusqu'à ce que la NSA les déclassifie en 1976. Onze innovations fondamentales (listées ci-dessous) sont directement liées aux travaux SIGSALY. De plus, SIGSALY fut le premier système de transmission numérique de la voix, le premier système de traitement du signal en temps réel, et le précurseur de tous les systèmes de traitement numérique du signal modernes.

1. Transmission d'un signal vocal quantifié
2. Téléphonie chiffrée inviolable
3. Transmission de la voix par PCM
4. Compression PCM par conversion analogique/numérique logarithmique
5. « *Frequency Shift Keying* » (FSK) multiniveaux
6. Réduction de la bande passante d'un facteur 10
7. « *Frequency Division Multiplex* » (FSK-FDM) sur un canal atténué
8. Diagramme en œil multiniveaux pour ajuster les intervalles d'échantillonnage
9. Premier convertisseur analogique/numérique rapide
10. Quantification à deux étages (premier convertisseur analogique/numérique pipeliné)
11. Transmission à étalement de spectre

X. VOCODER, SIGSALY et traitement du signal en temps réel

Le VOCODER de Dudley reposait sur des techniques analogiques à base de tubes à vide pour extraire en temps réel 12 paramètres de la voix, puis reconstruire la voix à partir de ces 12 paramètres. SIGSALY ajouta la quantification au VOCODER, et chiffra les 12 paramètres quantifiés grâce à un additionneur modulo 6 et des clés parfaitement aléatoires.

Toutes ces opérations étaient effectuées en parallèle et en temps réel. Le VOCODER et SIGSALY parvinrent à compresser la voix par un facteur 10 avec un chiffrement inviolable, longtemps avant l'invention de nos techniques numériques modernes. En fait, VOCODER et SIGSALY furent les premiers traitements numériques du signal en temps réel, tandis que les transformées de Fourier rapides (FFT), le DSP et les codecs n'apparurent que dans les années 1970. SIGSALY (et ses successeurs de la guerre froide) n'ont jamais été cassés par l'ennemi. Les transmissions ressemblaient à du bruit pour les Allemands et pour les Russes.

REMERCIEMENT

L'auteur souhaite remercier son ami pour son soutien, ses traductions et ses suggestions : le Général (2s) Jean-Louis Desvignes, Armée de Terre, Directeur du SCSSI, Directeur de l'ESAT, Président de l'ARCSI.