

Operation Rubicon

Analyse Cryptographique des Machines Crypto AG

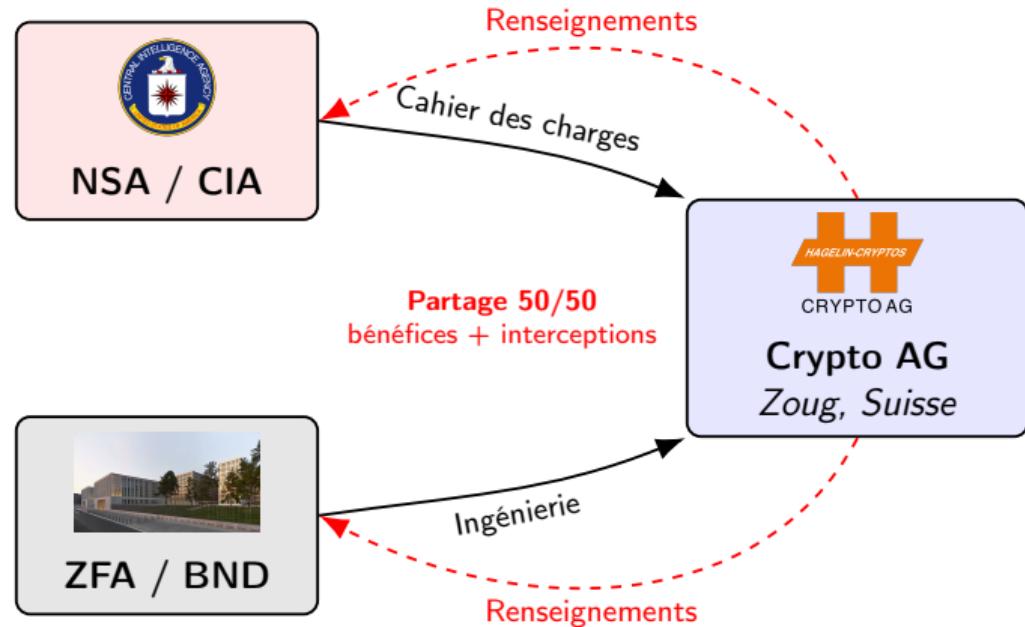
Arnaud Gomes

Université de Bordeaux

27 février 2026

L'Opération Rubicon (Thesaurus)

- Accord secret signé en 1970.
- Achat de Crypto AG via des sociétés écrans au Liechtenstein.
- Partage à 50/50 des bénéfices... et des interceptions diplomatiques.



[Vidéo : Sylvqin, L'Affaire Crypto AG, 2021]

Le Couvert de la Neutralité Suisse

Leader mondial du chiffrement matériel (ex : HC-520, HC-570). Vendu à +120 pays sous couvert de stricte neutralité.

Le Mécanisme Commercial :

- **Machines Dédiées** : Boîtiers électromécaniques lourds.
- **Boîte Noire** : Algorithmes propriétaires hardware non-documentés ("Security by Obscurity").
- **Légitimité** : Promesse de sécurité mathématique par Boris Hagelin.



Une machine de la gamme électronique HC-500.

Version A : "Alliés"

- États-Unis, Royaume-Uni, OTAN.
- Machines totalement sécurisées.
- Algorithme robuste non-compromis.

Version B : "Le Reste du Monde"

- Iran, Libye, Argentine, Inde, Vatican...
- Machines comportant la backdoor implantée par la NSA.
- Messages lisibles en temps réel par NSA/BND.

Même les ingénieurs et commerciaux de Crypto AG (ex : Hans Bühler en Iran) ignoraient manipuler des versions truquées.

Cas n°1 : La Guerre des Malouines (1982)

- **Le Contexte** : Conflit armé entre le Royaume-Uni et l'Argentine (cliente de Crypto AG, "Version B").
- **L'Exploitation** : La junte militaire argentine chiffrait l'intégralité de ses communications navales tactiques avec des machines de la série électronique HC-500.
- **Résultat Opérationnel** : La NSA déchiffre les positions navales argentines en temps réel et transmet les renseignements à Londres via les accords Five Eyes.

Asymétrie du Renseignement

L'Argentine, pensant son canal diplomatique sécurisé, négociait publiquement aux Nations-Unies tout en planifiant des frappes. Le Royaume-Uni, bénéficiaire des interceptions NSA/BND, disposait d'un avantage informationnel décisif.

Cas n°2 : Espionnage étatique et Anti-terrorisme (Années 70-80)

Crise des otages en Iran (1979)

- Crise diplomatique : 52 américains retenus à Téhéran.
- Jimmy Carter (USA) observe la diplomatie ennemie en temps réel via l'interception des HC-500 iraniennes.

Attentat "La Belle" Berlin (1986)

- Ronald Reagan accuse Mouammar Kadhafi de l'attentat de Berlin-Ouest.
- Preuve formelle : les télexes de "félicitations" libyens chiffrés par Crypto AG ont été déchiffrés quasi-instantanément par l'infrastructure de la NSA, fournissant un accès direct au texte clair.

Conséquence globale : durant toute la Guerre Froide, la CIA a intercepté les communications de plus de 120 pays de manière systématique.

[Vidéo : Sylvqin, L'Affaire Crypto AG, 2021]

Modèle (Cours Chap. II, Sect. 3)

Les machines Crypto AG utilisent un **chiffrement par flot synchrone**. Le message clair m_t est chiffré bit à bit avec la suite chiffrante z_t :

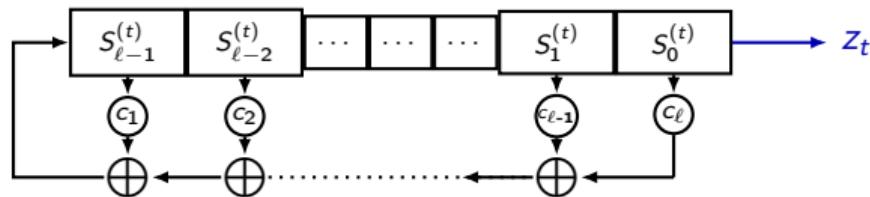
Équation Fondamentale

$$c_t = m_t \oplus z_t$$

Pourquoi en hardware (1970–1990) ?

- Implémentation en portes logiques extrêmement compacte.
- Symétrie : déchiffrement identique ($m_t = c_t \oplus z_t$).
- Pas de propagation d'erreur sur ligne radio/télex.

La suite chiffrante est produite par un **LFSR** (Linear Feedback Shift Register) : un automate linéaire sur \mathbb{F}_2 .



- **État** : $S^{(t)} = (S_0^{(t)}, \dots, S_{\ell-1}^{(t)}) \in \mathbb{F}_2^\ell$ (Def. II-4)
- **Mise à jour** : Récurrence linéaire sur \mathbb{F}_2 .
- **Polynôme de rétroaction** : $f(X) = 1 \oplus c_1X \oplus \dots \oplus c_\ell X^\ell$.
- **Période** : $T = 2^\ell - 1$ (m-suite, si f primitif). (Prop. II-5)

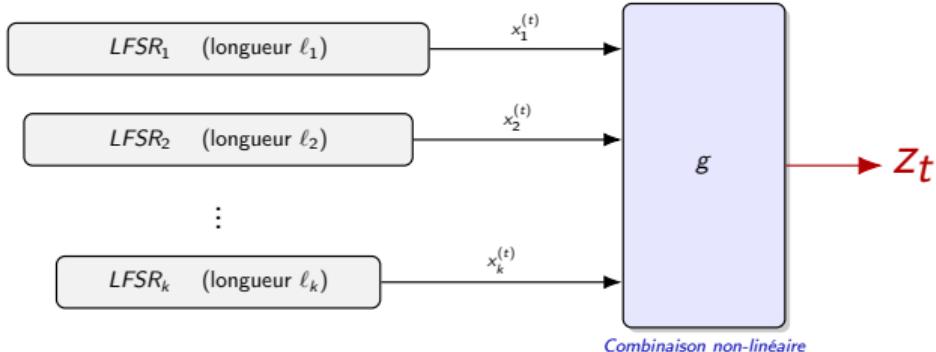
La Linéarité tue la Sécurité

Un LFSR brut est régi par des équations linéaires sur \mathbb{F}_2 . Son polynôme est reconstructible.

L'Algorithme de Berlekamp-Massey :

- Reconstruit le polynôme minimal $f(X)$ d'une suite récurrente linéaire.
- Complexité : $\mathcal{O}(\ell^2)$ opérations sur \mathbb{F}_2 .
- Il suffit d'observer 2ℓ bits consécutifs de la suite chiffrante z_t pour retrouver $S^{(0)}$ et prédire toute la suite.

Pour vendre une machine “inviolable”, Crypto AG devait briser cette transparence algébrique.



On combine k LFSRs **indépendants** via une fonction non-linéaire g .

Propriétés du Générateur

- **Génération** : $z_t = g(x_1^{(t)}, \dots, x_k^{(t)})$
- **Période Maximale** : Les ℓ_i sont premières entre elles.
- **Résultat** : $T_{tot} = \prod_{i=1}^k (2^{\ell_i} - 1)$.

[Modèle : Pornin, SSTIC]

La NSA conçoit en secret une fonction g biaisée gravée en silicium. Le combinateur échoue sciemment à satisfaire le critère d'**immunité de corrélation**.

Le Biais Exploitable

Il existe un registre $LFSR_1$ et un biais $\epsilon > 0$ tel que :

$$P(z_t = x_1^{(t)}) = 0.5 + \epsilon$$

Conséquence : La suite chiffrante z_t “fuite” de l'information sur la sortie $x_1^{(t)}$ d'un registre individuel.

Ce biais est invisible à l'usage quotidien, mais statistiquement exploitable avec suffisamment de chiffré.

[Biais ϵ : CCC, Reverse-Engineering 2020]

Le biais ϵ permet d'attaquer chaque registre L_i **indépendamment**.

Brute Force (sans backdoor)

$$\mathcal{O}(2^{\sum_{i=1}^k \ell_i})$$

Espace joint
Incalculable (siècles).

Corrélation (Backdoor)

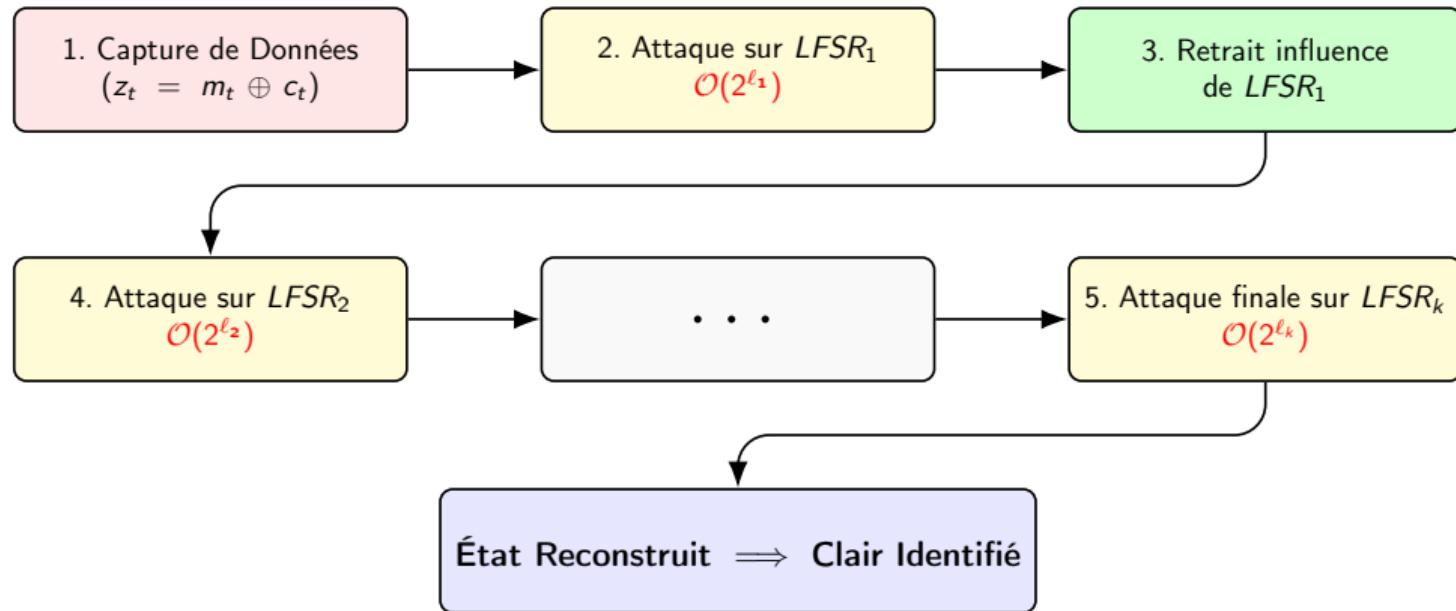
$$\mathcal{O}(\sum_{i=1}^k 2^{\ell_i})$$

Registres isolés
Quelques secondes.

Méthode : Avec du *clair probable* (en-tête diplomatique, salutation standard), l'attaquant compare statistiquement chaque état candidat de L_1 à la suite chiffrante captée. Le vrai état se démarque par corrélation.

[KPA Methodology : Pornin, SSTIC]

Visualisation de l'Attaque en Cascade



Complexité Totale : $\mathcal{O}(\sum_{i=1}^k 2^{\ell_i}) \ll \mathcal{O}(2^{\sum_{i=1}^k \ell_i})$

[Cascade Iteration : CCC, 2020]

Une ingénierie trop brillante

- **Mengia Caflisch**, ingénierie chez Crypto AG, analyse les générateurs HC-500.
- Elle identifie des **faiblesses statistiques suspectes** dans les combinateurs non-linéaires.
- Elle conçoit un **algorithme robuste** pour remplacer le générateur compromis.

Le Rôle de Widman

Widman justifiait académiquement les algorithmes affaiblis. Le haut degré algébrique apparent de g masquait la vulnérabilité statistique lors des revues internes.

La Contre-Attaque de la CIA

- La CIA panique : un algorithme robuste neutraliserait la backdoor.
- **Faux audit académique** par K-O. Widman (alias « Henry »), mathématicien recruté par la CIA.
- Widman invalide le travail de Caflisch et maintient les algorithmes affaiblis.

La Leçon

Même une ingénierie compétente à l'intérieur de l'entreprise n'a pas pu briser le cloisonnement.

[Vidéo : Sylvqin, L'Affaire Crypto AG, 2021]

L'Arrestation en Iran

- Hans Bühler, ingénieur commercial star de Crypto AG, est arrêté à Téhéran en **mars 1992**.
- Interrogé pendant **9 mois** par les services iraniens, libéré en **janvier 1993**.
- Le gouvernement iranien suspecte l'équipement d'être compromis suite à des fuites liées à des assassinats politiques.

L'Opération Démasquée

- Le **BND** paie la rançon/caution de **1 M \$** à l'Iran ; la **CIA** refuse de contribuer.
- Ce différend financier provoque le *Divorce Agreement* de 1993 : la CIA rachète la part du BND pour **17 M \$**.
- Crypto AG licencie Bühler ; l'attention médiatique fait s'écrouler le mythe de la “neutralité suisse”.

Ce n'est pas un audit cryptographique qui révèle la faille, mais une erreur humaine et un différend financier entre agences de renseignement.

[Vidéo : Sylvqin, L'Affaire Crypto AG, 2021]

L'Enquête #CRYPTOLEAKS (Février 2020)

- Enquête conjointe du *Washington Post*, *ZDF* et *SRF*.
- Documents CIA déclassifiés : contrôle de +40% des flux cryptés mondiaux (1970–1993).
- Rapport interne CIA : « **Le coup de maître du renseignement du siècle** ».

Épilogue

- Crypto AG dissoute en **2018**, scindée en deux entités.
- Le scandale relance le débat sur le chiffrement propriétaire vs. open-source.



Série HC-500 réputée mathématiquement inviolable.

[Vidéo : Sylvqin, L'Affaire Crypto AG, 2021]

- **Support de Cours :**

- G. Castagnos, *Cours de Cryptologie 2025-2026*, Univ. Bordeaux.
- Chap. II, Sect. 3 : Chiffrements par flot, LFSR (Def. II-4, Prop. II-5), Berlekamp-Massey (Def. II-8 et Prop. II-9), immunité de corrélation.

- **Sources Historiques & Techniques :**

- G. Miller, « *The intelligence coup of the century* », Washington Post, 2020.
- T. Pornin, « *The Swiss Cheese of Cryptography* », SSTIC.
- J. Gressel & CCC, Reverse-Engineering HC-7000, #CRYPTOLEAKS, 2020.
- Sylvqin, “*L’Affaire Crypto AG : la plus grande opération d’espionnage du siècle*”, YouTube, 2021.

Questions ?

« *Trust, but Verify.* »

– **Ronald Reagan**, sommets nucléaires (1987)

Ou plutôt : « *Don't trust. Open-Source everything.* »