

# Operation Rubicon

## Analyse Cryptographique des Machines Crypto AG

Arnaud Gomes

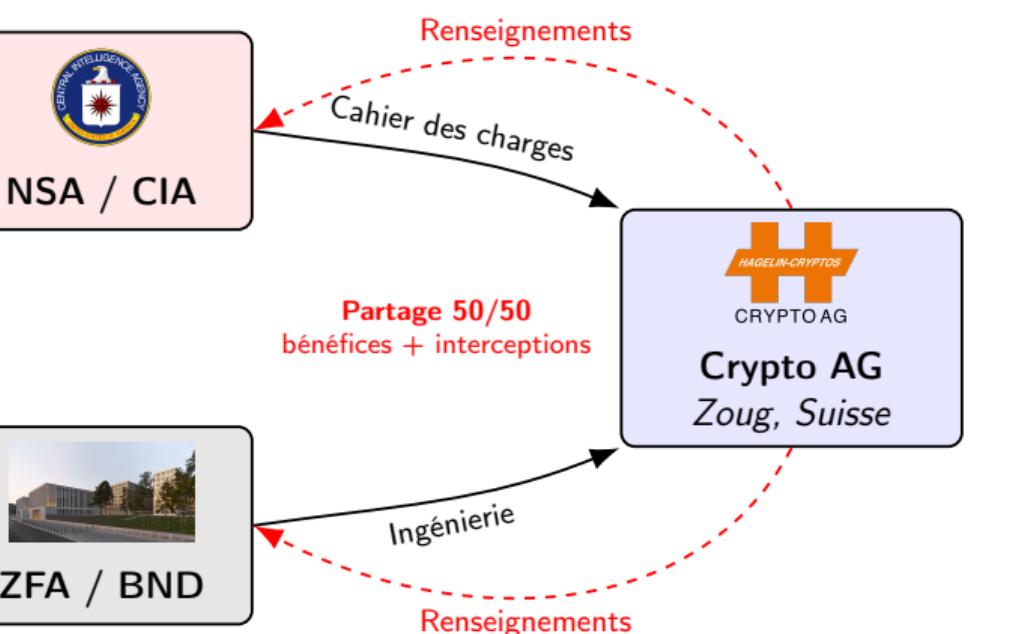
Université de Bordeaux

26 février 2026

- **Sujet** : Plus grande opération d'espionnage crypto du XXe siècle.
- **Acteurs** : CIA + BND possèdent secrètement Crypto AG (leader mondial chiffrement) pendant 50 ans.
- **Cible** : Équipements vendus à diplomates et gouvernements du monde entier.
- **Nature de la faille** : Pas une erreur de code ; backdoor mathématique implantée au niveau matériel.
- **Objectif** : Affaiblir l'espace des clés de multiples gouvernements.

## 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]

- **Date clé** : 1970, Guerre Froide ; accord secret "Thesaurus" (rebaptisé Rubicon).
- **Montage** : Rachat de Crypto AG (Zoug, Suisse) via sociétés écrans au Liechtenstein.
- **Partage** : Bénéfices commerciaux 50/50 entre CIA et BND.
- **Point crucial** : NSA et ZFA imposent les algorithmes de chiffrement ; contrôle total de la chaîne de production.

## 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 type Hagelin CX-52.*

- **Neutralité suisse** : Aura politique ⇒ fournisseur idéal pour tous les gouvernements.
- **Hardware lourd** : Blocs physiques (Hagelin) considérés inviolables.
- **Boîte noire** : Algorithmes HC-500 gravés dans le silicium, aucune doc mathématique fournie.
- **Danger** : "Security by Obscurity" = concept fondamentalement vicié en cryptographie.

## 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.*

- **Double production** : Même machine, algorithme interne différent.
- **Version A** : OTAN / alliés ; chiffrement robuste non-compromis.
- **Version B** : Reste du monde (Iran, Libye, Argentine, Inde...) ; backdoor NSA implantée.
- **Résultat** : Câbles diplomatiques lisibles en clair par NSA/BND.
- **Cloisonnement** : Même les ingénieurs Crypto AG ignoraient la fraude ; seule une micro-cellule concevait la faille.

## 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 Hagelin CX-52 / 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 concret** : Guerre des Malouines, 1982.
- **Confiance aveugle** : Argentine chiffrait tout via Hagelin CX-52/HC-500 (Version B).
- **Compromission totale** : Canaux tactiques et stratégiques lisibles par la NSA.
- **Relais Five Eyes** : NSA déchiffre en temps réel ⇒ renseignements transmis à Londres.
- **Avantage décisif** : UK connaîtait positions navales argentines avant les frappes.

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

### Attentat "La Belle" Berlin (1986)

#### 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.

- Ronald Reagan accuse Mouammar Kadhafi de l'attentat de Berlin-Ouest.
- Preuve formelle : les télex 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]

- En février 2020, une enquête conjointe du *Washington Post* (USA), de la *ZDF* (ALL) et de *SRF* (SUI) dévoile l'entièreté du scandale.
- **Berlin 1986** : Attentat "La Belle" ; Reagan invoque des "preuves absolues".
- **Source secrète** : Câbles libyens ("Félicitations pour Berlin") déchiffrés quasi-instantanément via backdoor Crypto AG.
- **Bilan global** : Trafic diplomatique du bloc non-aligné systématiquement intercepté ; +120 pays compromis.

## 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

$$c_t = m_t \oplus z_t$$

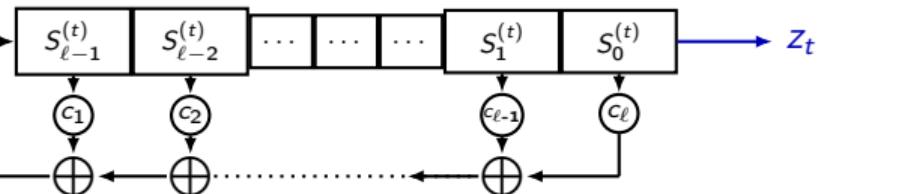
### Pourquoi en hardware (1970–1990) ?

- 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.

- **Réf. cours** : Chap. II, Sect. 3 : chiffrement par flot synchrone.
- **XOR** : Bit à bit  $\Rightarrow$  trivial en silicium.
- **Tolérance erreur** : 1 bit corrompu = 1 bit perdu (pas de propagation télex).
- **Clé de voûte** : Sécurité  $\equiv$  qualité de la suite chiffrante  $z_t$ .

# Le Générateur : LFSR

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)

- **Def. II-4** : LFSR = automate linéaire sur  $\mathbb{F}_2$ .
- **Prop. II-5** : Période max  $\iff$  polynôme primitif.
- **Sortie** :  $z_t = S_0^{(t)}$  (output direct du registre).
- **Limite** : Hardware efficace mais structure algébrique transparente.

- **Réf. cours :** Def. II-8 et Prop. II-9 (Berlekamp-Massey).
- **Coût :**  $2\ell$  bits observés  $\Rightarrow$  reconstruction complète de  $f(X)$  et  $S^{(0)}$ .
- **Verdict :** LFSR brut = sécurité nulle face à adversaire compétent.
- **Transition :** Nécessité d'introduire de la non-linéarité.

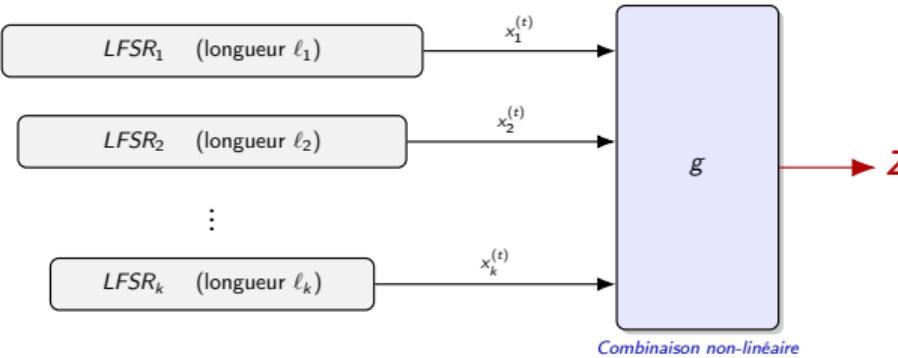
## La Linéarité tue la Sécurité

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  $2\ell$  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  $\ell_i$  sont premières entre elles.
- **Résultat :**  $T_{tot} = \prod_{i=1}^k (2^{\ell_i} - 1)$ .

- **Industrie :**  $k$  entre 3 et 6 LFSRs; ASIC compacts.
- **Longueurs  $\ell_i$  :** Premières entre elles  $\Rightarrow$  période globale  $= \prod(2^{\ell_i} - 1)$ , gigantesque.
- **Rôle de  $g$  :** Fonction non-linéaire censée rendre Berlekamp-Massey incalculable.
- **Astuce NSA :**  $g$  conçue pour paraître robuste, mais immunité de corrélation délibérément sacrifiée.
- **Conséquence :** Biais statistique  $\epsilon$  introduit  $\Rightarrow$  attaque par corrélation (Divide & Conquer) rendue possible.

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  $\epsilon$  : CCC, Reverse-Engineering 2020]

- **Backdoor** : Violation délibérée de l'immunité de corrélation de  $g$ .
- **Façade** :  $g$  suffisamment complexe pour résister à Berlekamp-Massey  $\Rightarrow$  aspect "sécurisé".
- **Faille cachée** : Immunité de corrélation sacrifiée  $\Rightarrow$  biais  $\epsilon$  exploitable.
- **Stratégie NSA** : Faiblesse statistique dissimulée derrière la complexité apparente de  $g$ .
- **Widman (alias « Henry »)** : Kjell-Ove Widman, mathématicien suédois recruté par la CIA, justifiait académiquement les algorithmes affaiblis auprès des ingénieurs suisses ; le haut degré algébrique apparent de  $g$  masquait la vulnérabilité statistique lors des revues internes.

Le biais  $\epsilon$  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)

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

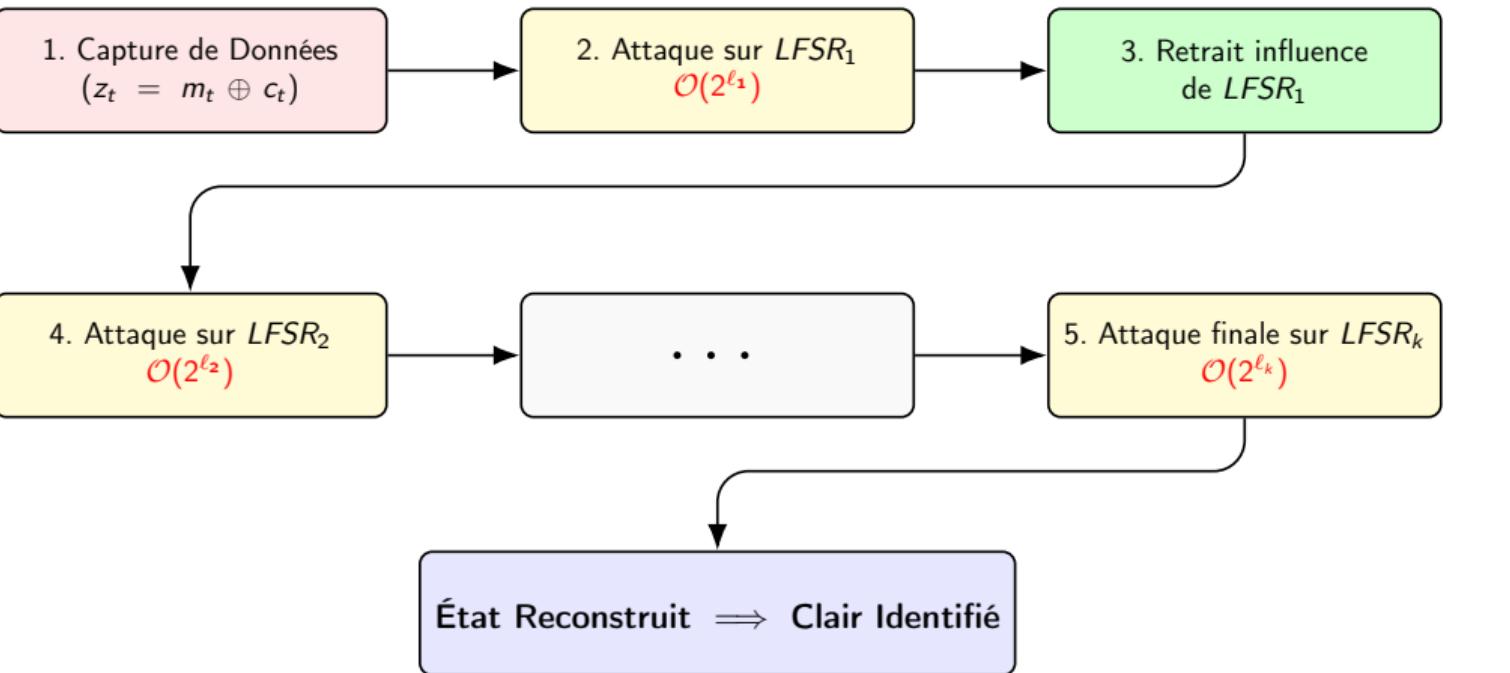
Registres isolés  
*Quelques secondes.*

- **Type** : Attaque à clair connu (KPA).
- **Source du clair** : En-têtes régulières télex diplomatiques (“To Mr Ambassador...”).
- **Récupération** :  $m_t \oplus c_t = z_t \Rightarrow$  suite chiffrante extraite.
- **Cascade** : Isoler  $LFSR_1$  via biais  $\epsilon_1$ , soustraire, attaquer  $LFSR_2$ , etc.
- **Gain** : Exponentielle de la somme → somme d'exponentielles.

**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



- **Principe :** Brise l'exposant (somme des longueurs) en somme linéaire.

- **Exemple :**  $k = 6 \Rightarrow$  quelques secondes vs. millénaires en brute-force.

- **Signal purifié :** Chaque étape soustrait l'influence des registres déjà cassés.

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]

## 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

### La Menace Interne

**Mengia Caflisch** : Ingénierie brillante de Crypto AG. Trouvant les générateurs suspects, elle conçoit un algorithme réellement robuste. La CIA panique et déploie un faux audit académique (via Kjell-Ove Widman (alias « Henry »)) pour étouffer son travail et sauver l'opération.

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

- **Ironie** : Pas un audit crypto qui révèle la faille, mais une erreur humaine.
- **Arrestation** : Mars 1992 ; Hans Bühler arrêté à Téhéran ; Iran suspecte les machines.
- **Interrogatoire** : 9 mois de détention ; Bühler ignorait la fraude.
- **Rançon** : BND paie 1 M\$ ; CIA refuse ⇒ peur de griller la couverture.
- **Divorce 1993** : CIA rachète part BND pour 17 M\$ ; contrôle exclusif.
- **Fuite médiatique** : Bühler alerte la presse ; lien Zoug-BND découvert.
- **Mengia Caflisch** : L'ingénierie qui a failli tout faire dérailler. Elle crée un code trop fort, obligeant la CIA à recourir au mathématicien K-O. Widman (alias « Henry ») pour neutraliser sa rustine.

## La Menace Interne

extbfMengia Caflisch : Ingénierie brillante de Crypto AG. Trouvant les générateurs suspects, elle conçoit un algorithme réellement robuste. La CIA panique et déploie un faux audit académique (via Kjell-Ove Widman) pour étouffer son travail et sauver l'opération.

## Le Coup de Maître

- Un rapport interne de la CIA décrit l'opération Rubicon



*Machine classique Hagelin réputée inviolable.*

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

- **Preuve formelle** : Février 2020 ; enquête Washington Post / ZDF / SRF (#CRYPTOLEAKS).
- **Documents CIA** : Déclassifiés ; prouvent contrôle de +40% des flux cryptés mondiaux (1970–1993).
- **Citation CIA** : “Coup de maître du renseignement du siècle”.
- **Liquidation** : Crypto AG dissoute en 2018.
- **Cause racine** : Décalage mathématique subtil sur un polynôme de LFSR.

- **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.

- **Fondements maths** : Chap. II (Castagnos) ; Def. II-4, Prop. II-5, Def. II-8, Prop. II-9.
- **Source primaire** : Documents CIA déclassifiés (Washington Post, 2020).
- **Technique** : Reverse-engineering CCC (Leipzig, 2020).

# Questions ?

« Trust, but Verify. »

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

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

- **Preuve définitive** : “Security by Obscurity” est un échec.
- **Risque matériel** : Hardware propriétaire non-audité = backdoor garantie.
- **La leçon** : Seuls les algorithmes publics (AES, NIST) audités résistent.
- **Clôture** : Merci ; questions sur LFSR, corrélation ou contexte géopolitique bienvenues.