

Operation Rubicon

Analyse Cryptographique des Machines Crypto AG

Arnaud Gomes

Université de Bordeaux

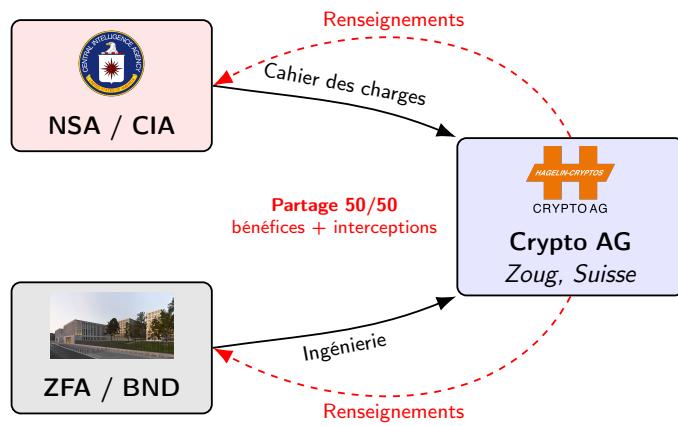
27 février 2026

- **Sujet** : Plus grande opération d'espionnage cryptologique dans l'histoire.
- **Acteurs** : CIA + BND pour la NSA pendant 50 ans.
- **Cible** : Équipements vendus par Crypto AG.
- **Nature de la faille** : Pas de faille au niveau matériel.
- **Objectif** : Affaiblir l'espace militaire et politique mondial.

Le Contexte : Le Partenariat CIA / BND

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 F
- **Montage** : Rachat de Cry
- **Partage** : Bénéfices comm
- **Point crucial** : NSA et Z chaîne de production.

Le Contexte : "Trusted" Hardware

- **Neutralité suisse** : Aura
- **Hardware lourd** : Blocs p
- **Boîte noire** : Algorithmes fournie.
- **Danger** : "Security by Ob

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.



Une machine de la gamme électronique HC-500.

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.

Le Contexte : Les Deux Versions (A et B)



- **Double production** : Même
- **Version A** : OTAN / allié
- **Version B** : Reste du monde
- **Résultat** : Câbles diplomatiques
- **Cloisonnement** : Même la micro-cellule concevait la

Version B : "Le Reste du Monde"

- Version A : "Alliés"
- États-Unis, Royaume-Uni, OTAN.
- Machines totalement sécurisées.
- Algorithme robuste non-compromis.

- 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.

L'Impact Historique : Exploitation des failles

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 concret** : Guerre des Malouines
- **Confiance aveugle** : Argentine
- **Compromission totale** : RSA
- **Relais Five Eyes** : NSA et BND
- **Avantage décisif** : UK contre l'Argentine

L'Impact Historique : L'Iran et la Libye



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.

- En février 2020, une enquête de SRF (SUI) dévoile l'enquête de l'attentat de Berlin 1986.
- **Berlin 1986** : Attentat "La Belle" Berlin (1986)
- **Source secrète** : Câbles interceptés quasi-instantanément via l'infrastructure de la NSA.
- **Bilan global** : Trafic diplomatique +120 pays compromis.

[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

$$c_t = m_t \oplus z_t$$

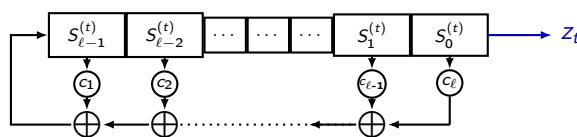
Pourquoi en hardware (1970–1990) ?

- 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.

- Réf. cours : Chap. II, Sect. 3
- XOR : Bit à bit \Rightarrow trivial
- Tolérance erreur : 1 bit d'erreur
- Clé de voûte : Sécurité égale

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** : $f(X) = 1 + c_1X + \dots + c_\ell X^\ell$.
- **Période** : $T = 2^\ell - 1$ (m-suite, si f primitif). (Prop. II-5)

- **Def. II-4** : LFSR = automate linéaire
- **Prop. II-5** : Période maximale
- **Sortie** : $z_t = S_0^{(t)}$ (output)
- **Limite** : Hardware efficacité

La Faiblesse : Berlekamp-Massey

La Linéarité tue la Sécurité

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

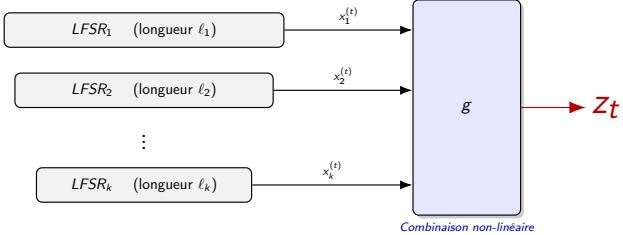
L'Algorithm de Berlekamp-Massey :

- 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.

- Réf. cours : Def. II-8 et F
- Coût : 2ℓ bits observés ⇒
- Verdict : LFSR brut = sé
- Transition : Nécessité d'i

La Solution : Générateur à Combinaison



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** : $T_{tot} = \prod_{i=1}^k (2^{\ell_i} - 1)$.

- **Industrie** : k entre 3 et 6
- **Longueurs ℓ_i** : Premières
- **Rôle de g** : Fonction non linéaire
- **Astuce NSA** : g conçue délibérément sacrifiée.
- **Conséquence** : Biais statistiques (Conquer) rendue possible.

La Backdoor Statistique de Crypto AG



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.

- **Backdoor** : Violation délibérée
- **Façade** : g suffisamment simple
- **Faille cachée** : Immunité de corrélation
- **Stratégie NSA** : Faibleless
- **Widman (alias « Henry »)** : CIA, justifiait académique haut degré algébrique app. internes.

L'Attaque : Divide & Conquer



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)

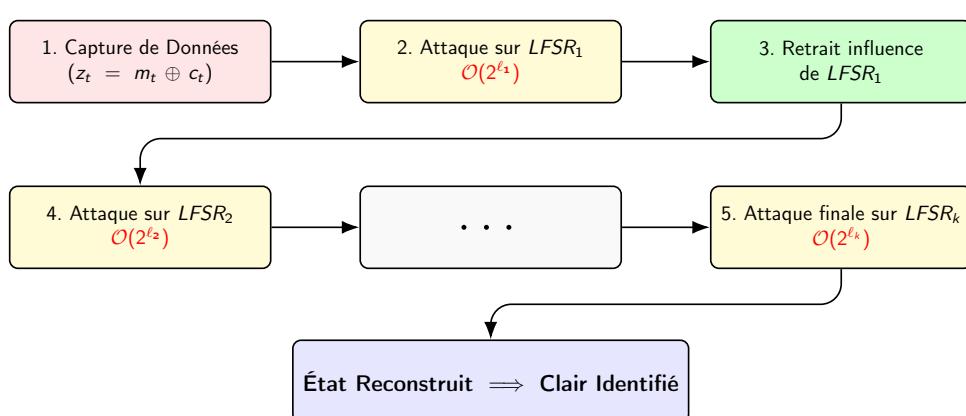
$$\mathcal{O}(\sum_{i=1}^k 2^{\ell_i})$$

Registres isolés
Quelques secondes.

- **Type** : Attaque à clair continu
- **Source du clair** : En-tête et corps de la mess
- **Récupération** : $m_t \oplus c_t = m_t$
- **Cascade** : Isoler $LFSR_1$ via $LFSR_2$
- **Gain** : Exponentielle de la longueur des registres

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.

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]

- **Principe** : Brise l'exposition
- **Exemple** : $k = 6 \Rightarrow$ quelque chose
- **Signal purifié** : Chaque étape

Années 1980 : La Menace Interne (Mengia Caflisch)

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.

- **Contexte** : Années 1980 ;
- **Découverte** : Elle repère un bug.
- **Initiative** : Elle conçoit une solution.
- **Réponse CIA** : Kjell-Ove Widman justifie ses choix.
- **Résultat** : La backdoor est conservée.
- **Ironie** : La menace la plus importante provient d'une employée consciente.

1992 : La Faille Humaine (L'Affaire Hans Bühler)



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]

- **Ironie** : Pas un audit cryp...
- **Arrestation** : Mars 1992 ;
- **Interrogatoire** : 9 mois d...
- **Rançon** : BND paie 1 M\$
- **Divorce 1993** : CIA rache...
- **Fuite médiatique** : Bühl...

2020 : La Déclassification et le Washington Post

Université
de BORDEAUX

- **Preuve formelle** : Février (#CRYPTOLEAKS).
- **Documents CIA** : Déclas (1970–1993).
- **Citation CIA** : “Coup de
- **Liquidation** : Crypto AG International.
- **Cause racine** : Décalage

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]

Références Bibliographiques

- **Fondements maths** : Ch
- **Source primaire** : Docum
- **Technique** : Reverse-engi

- **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 ?

- **Preuve définitive** : "Secure by design"
- **Risque matériel** : Hardware security
- **La leçon** : Seuls les algorithmes sont fiables
- **Clôture** : Merci ; questions ?

« Trust, but Verify. »

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

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