Operation Rubicon

Analyse Cryptographique de la Vulnérabilité Minerva

Arnaud Gomes

Université de Bordeaux

February 26, 2026

Bonjour à tous. Aujourd'hui je vais vous parler de l'une des plus grandes affaires d'espionnage du 20ème siècle : l'Opération Rubicon.

Pendant près de 50 ans, les agences de renseignement américaine (CIA) et ouest-allemande (BND) ont secrètement possédé la société suisse Crypto AG, qui était alors le leader mondial incontesté de la vente d'équipements de chiffrement et de sécurité des télécommunications pour les diplomates et tous les gouvernements.

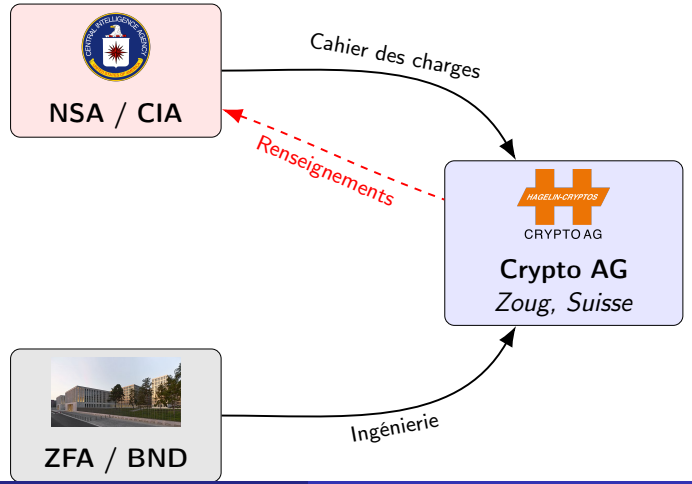
L'histoire que je vais vous raconter aujourd'hui montre que la vulnérabilité technique au sein de ces machines n'était pas une simple erreur de code. C'était une véritable porte dérobée (backdoor) mathématique, créée dès le départ pour écouter les communications du monde entier.

Le Contexte : Le Partenariat CIA / BND

université de BORDEAUX

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.



Pour bien comprendre la portée de cette attaque, je vais d'abord planter le décor. Tout commence en 1970, en pleine Guerre Froide. La CIA américaine et le BND d'Allemagne de l'Ouest signent un accord secret, nom de code Thesaurus, baptisé par la suite Rubicon.
Ils rachètent secrètement la société Crypto AG, basée à Zoug en Suisse, en utilisant un montage financier très complexe de sociétés écrans.
L'objectif de cette entité est double : d'une part les deux agences se partagent les énormes bénéfices commerciaux, environ 50/50. Mais surtout, je tenais à insister, la NSA et la ZFA (l'agence ouest-allemande) imposent désormais les algorithmes de chiffrement qui seront implantés dans les machines. Ils contrôlent la chaîne de production.

université de BORDEAUX

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.

Pourquoi le monde entier a-t-il acheté ces machines ? D'abord, à cause de la Suisse. Crypto AG bénéficiait de l'aura de neutralité politique, ce qui en faisait le fournisseur idéal.
Ensuite, le produit était matériel ("hardware"). Comme vous le voyez ici à droite avec les machines inventées par Boris Hagelin, il s'agissait de blocs lourds, considérés inviolables physiquement. Les algorithmes de la série Cryptomatic (HC-500) étaient gravés dans le silicium : aucune spécification ou documentation mathématique n'était fournie. C'est le principe même de la "Security by Obscurity", un concept très dangereux en cryptographie.

Le Contexte : Les Deux Versions (A et B)

université de BORDEAUX

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 faille *Minerva*.
- 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.

Ce que les pays clients ignoraient évidemment, c'est que l'usine de Zoug produisait deux versions de la même machine en modifiant juste l'algorithme interne.
La Version A, sécurisée organiquement, était vendue aux pays alliés de l'OTAN, comme le Royaume-Uni ou les Etats-Unis. La Version B était destinée au reste du monde : l'Iran, la Libye de Kadhafi, l'Argentine de la junte militaire, l'Inde... Ces machines contenaient la faille Minerva, permettant aux espions de lire les câbles diplomatiques en clair ou presque.
J'ai trouvé fascinant de voir que le degré de secret était tel que même les ingénieurs concepteurs de chez Crypto AG ignoraient qu'ils vendaient des boîtes truquées. Seule une micro-cellule d'ingénieurs mathématiciens concevait la faille pour la NSA !

L'Impact Historique : Exploitation des failles

université de BORDEAUX

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

- **Le Contexte :** Conflit armé entre le Royaume-Uni (Fournisseur "Version A") et l'Argentine (Client 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 l'ordre de bataille exact à Londres.

La trahison diplomatique parfaite

L'Argentine, pensant son canal diplomatique sécurisé, négociait publiquement aux Nations-Unies tout en planifiant des frappes. Margaret Thatcher lisait les télégrammes avant même le président argentin.

Pour bien comprendre comment ce niveau d'espionnage mathématique se traduit sur le terrain, je propose deux exemples historiques majeurs. D'abord, la Guerre des Malouines en 1982.
Lorsque l'Argentine envahit les îles, elle était totalement confiante dans ses communications chiffrées par ses machines Hagelin qu'elle jugeait ultra-modernes. L'erreur fut fatale. Le Royaume-Uni, pays ami des États-Unis et faisant partie de l'OTAN (donc utilisateur de la machine pure Version A), bénéficiait des écoutes totales.
Grâce à la faille Minerva, la NSA craquait en temps réel les communications navales et diplomatiques argentines. Elle transmettait la position des sous-marins et des frégates au commandement de Margaret Thatcher. Dans le monde des agences, on raconte que Londres lisait les plans de la junte militaire plus rapidement que les propres généraux argentins.

L'Impact Historique : L'Iran et la Libye

université de BORDEAUX

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 télégrammes de "félicitations" libyens chiffrés par Crypto AG explosent silencieusement dans les serveurs de la NSA.

Conséquence globale : Durant toute la Guerre Froide, la CIA a écouté plus de 120 pays sans la moindre résistance topologique.

Je voudrais également aborder le Moyen-Orient. Lors de la Révolution Iranienne de 1979 et de la crise des otages, le régime islamiste utilise massivement les HC-500 "Version B" léguées par le Shah d'Iran. Le président américain Jimmy Carter déchiffre jour par jour les discussions internes du gouvernement de l'Ayatollah Khomeini... alors même que ceux-ci négocient contre lui !
Plus tard, en 1986, lors de la bombe posée dans la discothèque berlinoise "La Belle", le président Ronald Reagan ordonne le bombardement de la Libye. Pour justifier cette frappe, l'administration américaine évoque des "preuves absolues". Ces preuves irréfutables s'avèrent être les câbles libyens chiffrés (des "Félicitations pour Berlin" envoyées de Tripoli) déchiffrés en quelques secondes par la NSA grâce, une fois de plus, à la faille intentionnelle de leurs machines suisses.
Pendant un demi-siècle, ce fut tout l'échiquier mondial de la Guerre Froide qui tombait, de manière transparente.

Modèle (Cours Chap. II – Def. II-1)

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) ?

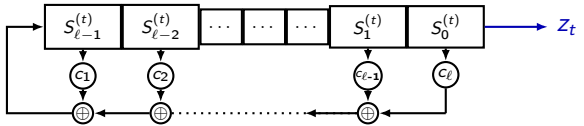
- Implémentation en portes logiques extrêmement compacte.
- Symétrie : déchiffrement identique ($m_t = c_t \oplus z_t$).
- Pas de propagation d'erreur sur ligne radio/télex.

- Def. II-1 : chiffrement par flot synchrone. - XOR bit à bit $\Rightarrow$ trivial en silicium. - Ligne télex : 1 bit corrompu = 1 bit perdu (pas de propagation). - Sécurité $\equiv$ qualité de la suite chiffrante z_t.

Le Générateur : LFSR

université de BORDEAUX

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



- **État** : $S^{(t)} = (S_0^{(t)}, \ldots, S_{\ell-1}^{(t)}) \in \mathbb{F}_2^\ell$ (Def. II-4)
- **Mise à jour** : Récurrence linéaire sur $\mathbb{F}_2$.
- **Polynôme de rétroaction** : $f(X) = 1 \oplus c_1 X \oplus \cdots \oplus c_\ell X^\ell$.
- **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. - Output : $z_t = S_0^{(t)}$ (sortie directe). - Hardware efficace, mais structure algébrique transparente.

université de BORDEAUX

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 :

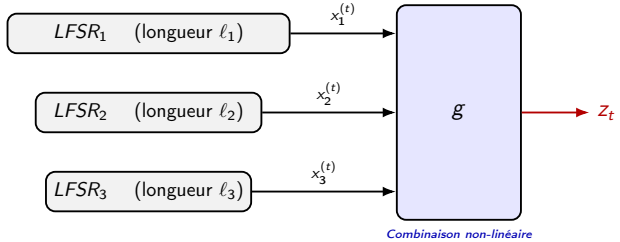
- Reconstruit le polynôme minimal $f(X)$ d'une suite récurrente linéaire.
- Complexité : $\mathcal{O}(\ell^2)$ opérations sur $\mathbb{F}_2$.
- Il suffit d'observer 2ℓ **bits** consécutifs de la suite chiffrante z_t pour retrouver $S^{(0)}$ et prédire toute la suite.

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

- Berlekamp-Massey : Thm. II-8. - 2ℓ bits de suite chiffrante $\Rightarrow$ reconstruction complète de $f(X)$ et $S^{(0)}$. - LFSR brut = sécurité nulle face à un adversaire compétent. - $\Rightarrow$ Nécessité d'introduire de la non-linéarité.

La Solution : Générateur à Combinaison

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



Générateur à Combinaison (Extension du Cours p.9)

$$z_t = g(x_1^{(t)}, x_2^{(t)}, \ldots, x_k^{(t)}) \qquad \text{où } g : \mathbb{F}_2^k \to \mathbb{F}_2$$

Critère de sécurité : g doit garantir l'**immunité de corrélation**.

- Architecture : k LFSR indépendants combinés par g (Modèle de Siegenthaler). - Réf Cours : Extension du concept de "LFSR filtré" (p.9) à une architecture multi-registres. - Argumentaire : Indispensable pour modéliser l'attaque Divide & Conquer sur Crypto AG. - Compromis de Siegenthaler : Ordre d'immunité de corrélation vs Degré algébrique. - Sécurité : Repose sur l'impossibilité d'isoler un registre via la suite chiffrante.

La NSA conçoit en secret une fonction g **biaisée** gravée en silicium. Le combineur 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.

- Minerva = violation délibérée de l'immunité de corrélation. - **Astuce NSA** : degré algébrique de g gardé élevé $\Rightarrow$ Berlekamp-Massey reste incalculable $\Rightarrow$ rassure les ingénieurs de Crypto AG. - Mais immunité de corrélation sacrifiée $\Rightarrow$ attaque par corrélation possible. - Compromis de Siegenthaler exploité à l'envers : la faiblesse est cachée derrière la complexité apparente.

L'Attaque : *Divide & Conquer*

université de BORDEAUX

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

Brute Force (sans backdoor)

$\mathcal{O}(2^{\ell_1+\ell_2+\ell_3})$

Espace joint
Incalculable (siècles).

Corrélation (Minerva)

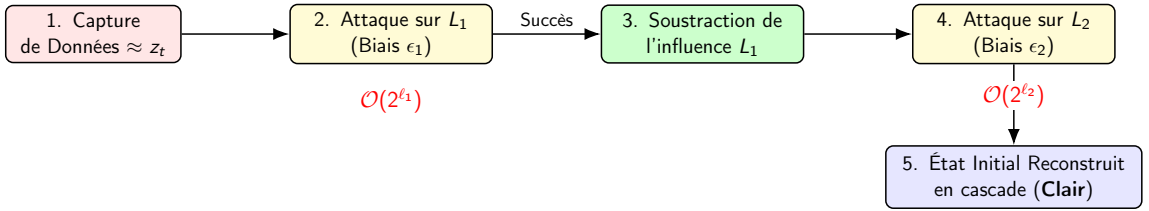
$\mathcal{O}(2^{\ell_1} + 2^{\ell_2} + 2^{\ell_3})$

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.

- **Attaque à clair connu**. - Source du clair : en-têtes régulières des télex diplomatiques ("To Mr Ambassador..."). - $m_t \oplus c_t = z_t \Rightarrow$ suite chiffrante récupérée. - Isoler $LFSR_1$ grâce au biais ϵ_1, soustraire, puis attaquer $LFSR_2$, etc. - Exponentielle de la somme $\rightarrow$ somme d'exponentielles.

Visualisation de l'Attaque en Cascade



Le processus itératif de l'attaque NSA :

1. Capter le chiffré cible, et y associer du "Clair probable" (en-tête télex, salutation diplomatique).
2. Simuler $LFSR_1$ pour toutes ses clés partielles (2^{ℓ_1} états).
3. Conserver la clé de $LFSR_1$ qui maximise la corrélation avec la suite chiffrante.
4. Soustraire l'influence de $LFSR_1$ et continuer sur les registres suivants.

- Attaque en cascade : chaque $LFSR_i$ est cassé séquentiellement. - Étape 1 : $c_t \oplus m_t = z_t$ (clair connu). - Étape 2 : brute-force sur 2^{ℓ_1} états de $LFSR_1$, corrélation avec z_t. - Étape 3 : soustraire $x_1^{(t)}$, purifier le signal résiduel. - Itérer pour $LFSR_2$, $LFSR_3$ $\Rightarrow$ clé totale reconstruite.

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

université de BORDEAUX

L'Arrestation en Iran

- Hans Bühler, ingénieur commercial star de Crypto AG, est brusquement arrêté à Téhéran en 1992.
- Le gouvernement Iranien suspecte l'équipement d'être compromis suite à des fuites liées à des assassinats politiques.

L'Opération Démasquée

- La CIA et le BND refusent d'intervenir pour protéger la couverture.
- Crypto AG finit par payer une étrange rançon/caution de 1M $ à l'Iran, puis licencie Bühler.
- L'attention médiatique fait s'écrouler le mythe

La Couverture Parfaite

Bühler, comme l'immense majorité des ingénieurs suisses de Crypto AG, ignorait totalement la manipulation des schémas d'immunité des LFSR par Minerva !

Mais alors, si le système était mathématiquement pur en surface, comment l'empire secret Rubicon s'est-il finalement effondré ?

Ironiquement pour nous analystes d'algorithmes, ce n'est pas un audit cryptographique qui a révélé la faille, mais une grossière erreur humaine ! En 1992, Hans Bühler, un des vendeurs phares de Crypto AG qui vendait ces machines au Moyen-Orient, est brusquement emprisonné par l'Iran. Les iraniens s'étaient rendus compte que l'Ouest anticipait de manière trop miraculeuse leurs frappes terroristes et politiques, et ont logiquement pointé du doigt l'intégrité de ces machines suisses qu'on leur avait lourdement facturées.

Bühler, qui n'était pas au courant de la fraude, reste emprisonné neuf mois. La CIA a catégoriquement refusé de lever le petit doigt pour ne pas "griller" la couverture technologique. Dès sa libération sous caution, ce traitement injuste le poussera à alerter la presse germanique. De fil en aiguille, les journalistes d'investigation trouveront la relation cachée entre l'usine de Zoug et le BND à Munich. Le secret industriel du siècle venait de s'éteindre.

2020 : La Déclassification et le Washington Post

université de BORDEAUX

Le Secret Révélé (#CRYPTOLEAKS)

- En Février 2020, une enquête conjointe du *Washington Post* (USA), de la *ZDF* (ALL) et de *SRF* (SUI) dévoile l'entièreté du scandale.
- Ils publient des documents de la CIA déclassifiés, prouvant que de 1970 à 1993, la quasi-totalité des communications sécurisées mondiales étaient lues par la NSA.

Le Coup de Maître

- Un rapport interne de la CIA décrit l'opération Rubicon comme "Le coup de maître du renseignement du siècle".

Machine classique Hagelin réputée inviolable.

Pour conclure définitivement sur ce pan d'histoire, comment a-t-on la certitude absolue de la véracité de cette incroyable opération ?

En Février 2020 (il y a à peine quelques années), une enquête coup de poing mondiale entre le Washington Post, la télévision allemande et la télévision suisse ont publié ce qu'ils appellent les "Cryptoleaks". Des documents top-secrets de la CIA ont été déclassifiés, et ont formellement prouvé que de 1970 jusqu'à la fin de la guerre froide, ce duo contrôlait plus de 40% des flux mondiaux cryptés.

Un rapport interne de l'agence va même jusqu'à qualifier Rubicon de "coup de maître du renseignement du siècle". La société Crypto AG a finalement été liquidée en 2018. Des décennies de communications ultra-secrètes ont été aspirées silencieusement, le tout à cause d'un décalage mathématique subtil sur un polynome de LFSR.

Références Bibliographiques

- **Support de Cours :**
  - G. Castagnos, *Cours de Cryptologie 2025-2026*, Univ. Bordeaux.
  - Chap. II : Chiffrements par flot, LFSR, Berlekamp-Massey, 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.

- Fondements mathématiques : Chap. II (Castagnos), Def. II-4, Prop. II-5, Thm. II-8. - Source primaire : documents CIA déclassifiés, publiés par le Washington Post. - Aspects techniques : reverse-engineering par le CCC (Leipzig 2020).

Questions ?

"Trust, but Verify."

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

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

- L'Opération Rubicon est la preuve définitive que "Security by Obscurity" est une faille. - Confier des communications étatiques à du hardware propriétaire non-audité = backdoor garantie. - La leçon : seuls les algorithmes publics (AES, standards NIST) audités par la communauté offrent une sécurité réelle. - Merci. Questions bienvenues sur les LFSR, la corrélation, ou le contexte géopolitique.