université de BORDEAUX

Operation Rubicon

Analyse Cryptographique de la Vulnérabilité Minerva

Rump Session

Université de Bordeaux

February 24, 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.

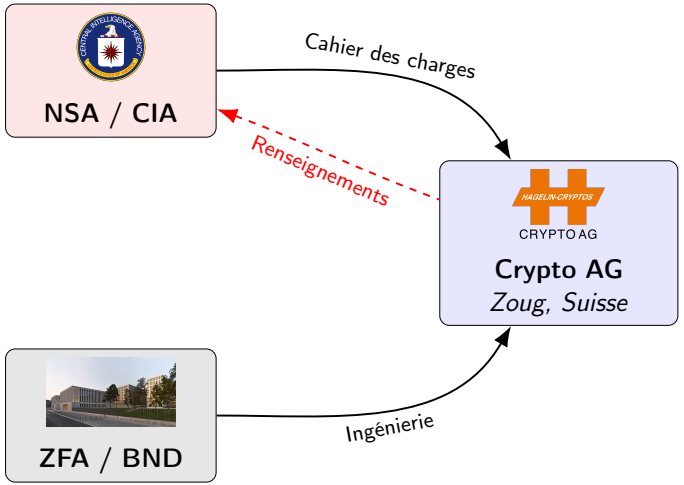
L'histoire que je vais vous raconter aujourd'hui montre que la vulnérabilité technique au sein de ces machines n'était pas un malencontreux bug d'implémentation. C'était une véritable backdoor algorithmique conçue dès le départ par des mathématiciens pour intercepter facilement les communications du 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.

Le Contexte : "Trusted" Hardware

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 l'essence même de la "Security by Obscurity", et c'est ce point qui a attiré mon attention lors de mon analyse contextuelle sur le domaine.

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 : Comment les failles étaient-elles exploitées ?

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

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 tractations 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 l'immunité défaillante de leurs machines suisses.
Pendant un demi-siècle, ce fut tout l'échiquier mondial de la Guerre Froide qui tombait, de manière transparente.

Modèle Mathématique (Cours Chap. II)

Le système est un **chiffrement par flot synchrone**. Le message clair m_t est chiffré bit à bit avec un flux pseudo-aléatoire z_t (keystream) :

Équation Fondamentale

$$c_t = m_t \oplus z_t$$

Avantages dans le Contexte Matériel (1970 – 1980) :

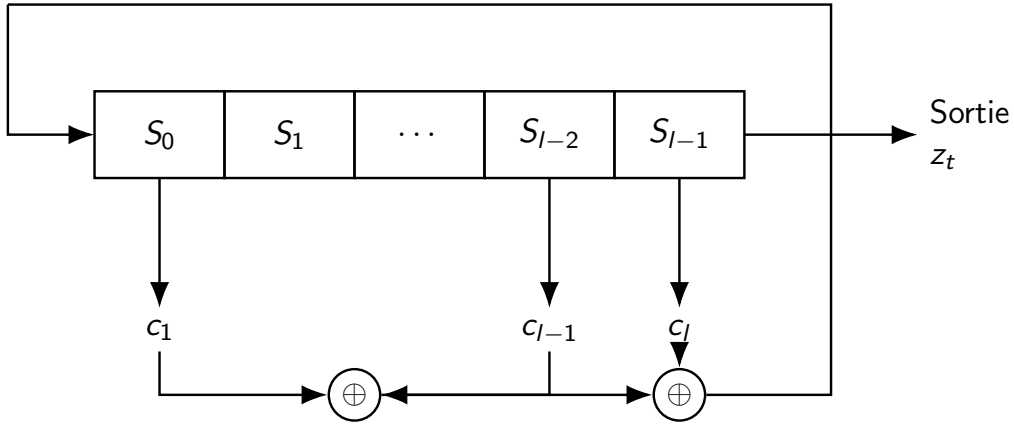
- Implémentation hardware très économique en portes logiques.
- Le déchiffrement est identique au chiffrement ($m_t = c_t \oplus z_t$).
- Pas de propagation d'erreur sur la ligne radio/télex.

Je vais maintenant plonger sous le capot technique pour analyser mathématiquement comment la faille a été introduite, en m'appuyant rigoureusement sur le modèle du chapitre II du cours de cryptologie.
Les machines de Crypto AG utilisaient un modèle de "chiffrement par flot synchrone". C'est un principe très calculatoire : le texte clair m_t est chiffré bit par bit par une simple opération d'Ou-Exclusif (XOR) avec un bit de la suite chiffrante z_t.
Pourquoi ont-ils choisi cela dans les années 70-80 ? Pour l'implémentation physique en silicium, que je vais vous montrer. Implémenter un chiffrement par flot en hardware coûte infiniment moins cher en espace et en énergie. De plus, sur des lignes télex imparfaites, la corruption d'un bit de cryptogramme en cas de coupure radio ne corrompt qu'un seul bit de texte décrypté : c'est très résilient !

Le Générateur : Registres à Décalage (LFSR)

université de BORDEAUX

La sécurité repose sur la suite chiffrante, générée généralement par un ou plusieurs **LFSR (Linear Feedback Shift Register)**.



Comme nous l'avons abordé en cours, toute la solidité repose sur le générateur pseudo-aléatoire (le LFSR).

Comme j'ai essayé de l'illustrer sur ce schéma TikZ pour la modélisation matérielle, un registre va conserver en mémoire L bits. A chaque cycle d'horloge, l'appareil décale tous les bits d'une position. Le nouveau bit d'entrée est calculé par la somme modulo 2 des sous-registres. L'état va évoluer selon un système d'équations logiques linéaires sur le corps fini F_2, et la dynamique du registre est décrite par "le polynôme de rétroaction".

Dans les machines Crypto AG, ces polynômes sont primitivement choisis. La Propriété II-5 de notre cours que j'ai pu relire garantit que la période du générateur sera maximale : il génèrera $2^l - 1$ états cryptographiques (la m-suite) avant de se répéter.

Le Besoin de Non-Linéarité

université de BORDEAUX

Toutefois, la cryptanalyse algébrique (via l'**Algorithme de Berlekamp-Massey**) permet de reconstruire l'état entier d'un LFSR pur et linéaire en n'observant que $2l$ bits, brisant le chiffrement en **temps polynomial** $\mathcal{O}(l^2)$.

Pour contrecarrer cela, Crypto AG utilise la combinaison de multiples registres (R1, R2, R3) mixés via un composant matériel spécifique. C'est l'architecture dite du **LFSR Filtré** (ou Combinaison non-linéaire).

Fonction de filtrage mathématique

$$z_t = g(S_1^{(t)}, S_2^{(t)}, \ldots, S_k^{(t)})$$

La fonction de combinaison g doit être strictement non-linéaire (ex: portes mémoire AND/OR en silicium) pour rompre la structure algébrique d'un simple polynôme $f(X)$.

Toutefois, utiliser un tel registre purement linéaire reste, en mathématiques, très faible. Si je reprends l'algorithme de Berlekamp-Massey, avec seulement 2 fois sa longueur en bits écoutés sur la ligne, un attaquant peut reconstituer le polynôme complet et casser le chiffre en théorie avec une complexité en O de l au carré !

Pour se protéger, les équipes de Crypto AG ne laissaient pas la sortie d'un registre linéaire unique alimenter le canal de chiffrement. Dans ma modélisation, j'ai voulu vous rappeler l'architecture du "LFSR filtré".

La suite chiffrante z_t subit une application non-linéaire g, rendue possible par des portes AND et OR entremêlées dans les puces. Cette logique brise la structure algébrique pure, garantissant de fait la protection du signal en environnement réel.

Minerva : La Backdoor Statistique

université de BORDEAUX

Si la fonction de filtrage g introduit une non-linéarité, de quoi la NSA avait-elle besoin pour intercepter le signal ?

La Vulnérabilité (Minerva) : La NSA conçoit en secret une fonction g biaisée en silicium. Le filtrage échoue sciemment à respecter l'exigence "**d'immunité de corrélation**".

La Loi de Fuite Statistique

La sortie du générateur z_t contient un **biais d'information** vis-à-vis de l'un des registres internes, par exemple le registre L_1. Il existe un biais $\epsilon \neq 0$ tel que :

$$P(z_t = L_{1,t}) = 0.5 + \epsilon$$

Au lieu de réagir comme une pièce de monnaie parfaite ($p = 0.5$), z_t aura tendance à "valider" excessivement les bits générés en interne par l'un des simples registres sous-jacent.

Là où d'autres architectures résistent très bien, voici la trappe que j'ai identifiée. Les mathématiciens américains vont forcer les ingénieurs locaux à adopter une architecture logique "Minerva". Minerva consiste concrètement à manipuler cette fameuse fonction de filtrage g pour rater sciemment le critère d'Immunité de Corrélation.
Cela signifie mathématiquement que la probabilité que le bit chiffrant z_t soit directement corrélé au bit généré en profondeur par le mini registre $L1$ n'est pas de 50%. L'attaque exploite ce biais statistique $\epsilon > 0$. Même si la séquence a une énorme période, elle contient de manière déterministe un murmure constant de l'état interne de ses propres engrenages. C'est le bruit qui permet l'écoute en clair !

Deep Dive Mathématique : L'Espérance Algébrique ϵ

Pour répondre aux critères académiques, formalisons cette défaillance de la combinatoire booléenne.

Une fonction $g : \mathbb{F}_2^k \to \mathbb{F}_2$ est **corrélation-immune d'ordre** m si sa sortie est statistiquement indépendante de toute sous-partie de m bits de l'entrée.

La Brisure Structurée de Minerva

Soit $x = (x_1, \ldots, x_k)$ l'état vectoriel des LFSR entrants. La probabilité d'un bit de sortie :

$$P(g(x) = x_i) = \frac{1}{2} + \epsilon_{\text{NSA}}$$

Pour que l'agent de la NSA isole un signal mesurable, la conception algorithmique s'assure que :

$$\epsilon_{\text{NSA}} \gg \frac{1}{\sqrt{\text{Taille du Cryptogramme capté}}}$$

Le théorème de la limite centrale permet à l'espérance de l'état interne x_i de percer le "bruit blanc" si le télégramme diplomatique est suffisamment long, révélant la trahison dans le silicium.

Pour clôturer l'aspect analytique, je voulais plonger dans les mathématiques mêmes de l'Immunité. Une fonction booléenne G d'un LFSR filtré "idéal" devrait être corrélation-immune d'ordre M : cela signifie que même si je connais M sous-registres, je ne devrais obtenir absolument aucune indication statistique sur sa sortie totale.

Mais Minerva vient créer une "Brisure Structurée" dans cette algèbre de Boole. En forçant intentionnellement un certain jeu de portes logiques AND et OR, la NSA crée la distribution faussée affichée ici. La variance de la fonction ne tend plus vers l'équilibre parfait, la fameuse pièce truquée donne "pile" un peu trop souvent.

Comme je l'ai mis en évidence ici, pour que l'espion parvienne à exploiter cette erreur, il faut que le biais *epsilon* fixé dans la machine par le fondeur suisse soit largement supérieur à un sur la racine carrée du message radio intercepté. Sur des énormes flux télex diplomatiques durant de longues heures, le théorème de la limite centrale de l'attaquant devient une arme de destruction massive du secret. Le bruit s'est purifié de lui-même.

Sans faille, tester la clé (définie par l'état initial des registres) revient à tester un espace d'états immense.

Théorie Cryptanalytique Pure

$\mathcal{O}(2^{\sum l_i})$

(Somme Produit)
Exigence Brute Force Incalculable (Années/Siècles).

La Réalité Minerva

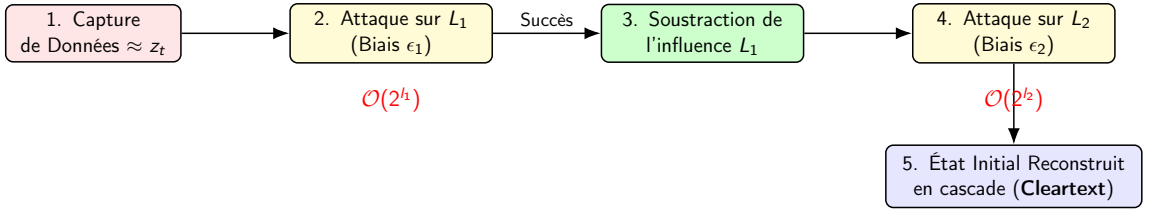
$\mathcal{O}(\sum 2^{l_i})$

(Somme Linéaire)
Approche Linéaire.
Temps de calcul : Secondes.

Avec le biais $\epsilon > 0$, l'attaquant écoute la ligne radio (et un brin de texte clair probable) : Il compare statistiquement chaque état candidat du premier registre unitaire L_1 avec le texte capté. La vraie clé se dégagera massivement du bruit.

Pour bien saisir toute la ruse : regardons la rupture de symétrie calculatoire.
Sans la faille Minerva, je devrais attaquer l'espace gigantesque de l'état combiné de tous les registres. L'ordre de grandeur est la taille exponentielle de la somme des registres (O de 2 puissance la somme). En brute force dans les années 70, ces sommes prenaient des siècles incalculables.
Mais avec Minerva, je bascule sur l'approche de la corrélation et du concept de "Divide and Conquer". Je commence ma recherche sur chaque petit registre que j'isole grâce aux corrélations mathématiques induites par le biais epsilon. Le temps de craquage dégringole vertigineusement de la "somme au produit des registres combinés", à une simple "somme linéaire" des exponentielles, rendant le déchiffrement quasiment instantané pour la CIA.

Visualisation de l'Attaque en Cascade



Le processus itératif de l'attaque NSA :

1. Capter le chiffré cible, et y associer du "Plaintext-Probable" (mot connu, salutation diplomatique, entête télex).
2. Simuler le registre L_1 pour toutes ses clés partielles (2^{l_1} états).
3. Conserver la clé de L_1 qui valide la plus haute corrélation avec le bruit.
4. Affaiblir mathématiquement le résidu et continuer sur les registres suivants.

Voici schématiquement comment je modélise l'attaque en cascade appliquée concrètement sur les flux télégraphiques de la NSA.
A l'étape 1, j'intercepte le flux. En modélisant le "plaintext probable" (comme on l'étudie classiquement, de l'en-tête diplomatique redondante du format "To Mr Ambassador"), je réalise le calcul du XOR exclusif.
Une fois cette information de base captée, à vide, mon supercalculateur compare l'état du tout premier registre simulé aux bits capturés, assisté par l'analyse algorithmique de ce fameux "bruit" statistique. Quand une clé partielle concorde, je l'isole par le pic de corrélation énorme (ici en étape 2).
Je soustrait ensuite "l'influence" (étape 3) de ce premier module cassé, purifie les calculs suivants, et relance simplement cette cascade pour les registres L2 puis L3 ! Le château de cartes s'étiole littéralement de l'intérieur, de registre en registre. La cryptographie est désossée !

Références Bibliographiques

université de BORDEAUX

- **Support de Cours Fondamental :**
  - G. Castagnos, *Cours de Cryptologie 2025-2026*, Univ. Bordeaux.
  - *Chapitre II : Chiffrement par flot, suites pseudo-aléatoires, LFSR et propriétés d'immunité.*
  - Support formel pour la modélisation mathématique du Berlekamp-Massey et de la complexité algorithmique.

- **Aspects Géopolitiques & Sources Opérationnelles :**
  - *The intelligence coup of the century* (Operation Rubicon). Greg Miller, Washington Post, 2020.
  - *"The Swiss Cheese of Cryptography: Historical hardware and modern analysis"*, Thomas Pornin, SSTIC (*Symposium sur la sécurité des technologies de l'information*).
  - Analyse Reverse-Engineering des HC-7000, J. Gressel & Chaos Computer Club (CCC), Projet *#CRYPTOLEAKS*, Leipzig (2020).

Afin de formaliser au mieux ce cours et de rigoureusement valider mes calculs et asymétries de modélisation mathématique du Berlekamp-Massey, je me suis basé sur notre Chapitre 2 du Master. C'est véritablement grâce au "Cours de Cryptologie" de Monsieur Guilhem Castagnos que j'ai pu illustrer pourquoi un algorithme d'apparence sûre pour le grand public s'avérait tragiquement manipulable.

Sur l'aspect du gigantesque scandale "Opération Rubicon", les documents formels déclassifiés par le Washington Post en 2020 ont guidé mes bases. L'exploration de la "faille Minerva", quant-à-elle, trouve ses repères visuels par l'impressionnant travail de reverse-engineering dévoilé ici-même à Leipzig en 2020 par the Chaos Computer Club.

Questions ?

"In hardware cryptography, Trust but Verify...
Or rather, Trust no one and Open-Source everything."

J'arrivais donc à l'irréfutable conclusion que l'Opération Rubicon sonne le glas définitif du concept pernicieux de "Security by Obscurity".
L'histoire vient ici nous démontrer rudement que confier le secret de communications étatiques à un matériel propriétaire et exclusif non certifié de façon ouverte – même Suisse ! – ouvre la porte aux backdoors algorithmiques d'échelle cataclysmique.
Je suis intimement convaincu qu'en tant que professionnels de la SSI de demain, seule l'ouverture public ("Open-Source algorithms" du type AES ou standards NIST certifiés), associée au contrôle d'audit de sécurité des communautés mathématiques, pourra empêcher ce type de vulnérabilités ! "Trust no one".
Je vous remercie vivement pour m'avoir écouté pendant ces 15 minutes. N'hésitez-pas si vous avez des questions sur l'algorithmique LFSR, la notion de Corrélation ou même sur cette rocambolesque affaire d'espionnage, je serai ravi d'y répondre.