

- **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.

- **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.

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

- **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 concret** : Guerre des Malouines, 1982.
- **Confiance aveugle** : Argentine chiffrait tout via série 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 connaissait positions navales argentines avant les frappes.

- 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.

- **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 .

- **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** : 2ℓ 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.

- **Industrie** : k entre 3 et 6 LFSRs ; ASIC compacts.
- **Longueurs** ℓ_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 ϵ introduit \Rightarrow attaque par corrélation (Divide & Conquer) rendue possible.

- **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 ϵ 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.

- **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 ϵ_1 , soustraire, attaquer $LFSR_2$, etc.
- **Gain** : Exponentielle de la somme → somme d'exponentielles.

- **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.

- **Contexte** : Années 1980 ; Caflisch travaille sur les générateurs HC-500.
- **Découverte** : Elle repère des biais statistiques dans le combinateur g .
- **Initiative** : Elle conçoit un algorithme robuste de remplacement.
- **Réponse CIA** : Kjell-Ove Widman (alias « Henry ») mène un faux audit pour invalider son travail.
- **Résultat** : La backdoor est préservée ; Caflisch ne sera jamais informée de la vérité.
- **Ironie** : La menace la plus sérieuse pour l'opération ne vient pas d'un adversaire, mais d'une employée consciencieuse.

- **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.

- **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, scindée en CyOne Security et Crypto International.
- **Cause racine** : Décalage mathématique subtil sur un polynôme de LFSR.

- **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).

- **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.