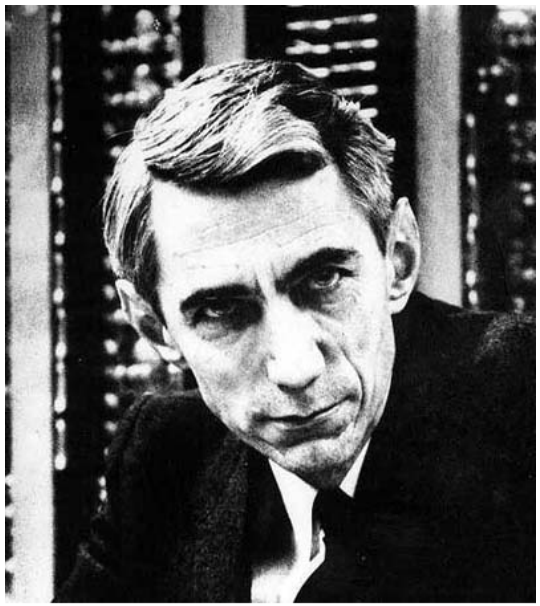
Analyse algébrique en cryptographie

Luk Bettale
Jean-Charles Faugère, Ludovic Perret

Équipe SALSA
LIP6, Université Paris 6 & INRIA Paris-Rocquencourt

Contexte Général

"Breaking a good cipher should require as much work as solving a system of simultaneous equations in a large number of unknowns of a complex type."
(Communication Theory of Secrecy Systems, 1949)



Claude E. Shannon

Cryptanalyse algébrique (1)

Objectif

Analyse de la sécurité – Problème fondamental en cryptologie

Démarche en 2 étapes

1. Mise en équation sous forme d'un système algébrique
2. Résolution du système (ou à défaut estimation de la difficulté)

Stratégie :
Minimiser le nombre de variables et le degré des équations

Cryptanalyse algébrique (2)

Outils puissants pour résoudre des systèmes.
$\Rightarrow$ base de Gröbner

Cryptosystème

Base de Gröbner

$$x + 1 = 0$$
$$y + t + 1 = 0$$
$$z + t = 0$$
$$t^2 + t = 0$$

$$x + xy + xz + yz + yt + zt + t = 0$$
$$xz + xt + yz + y + zt + 1 = 0$$
$$xy + xt + zt + t + 1 = 0$$
$$x + xy + xz + yz + yt + zt + z = 0$$

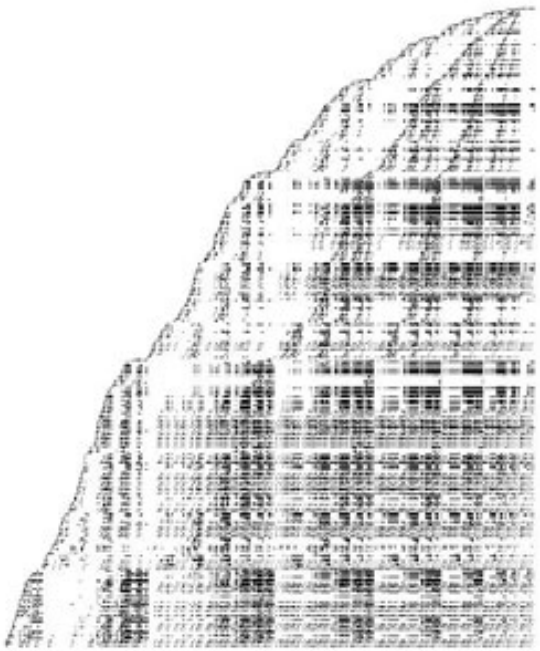
Système d'équations

$x = 1$	$x = 1$
$y = 0$	$y = 1$
$z = 1$	$z = 0$
$t = 1$	$t = 0$

Solutions

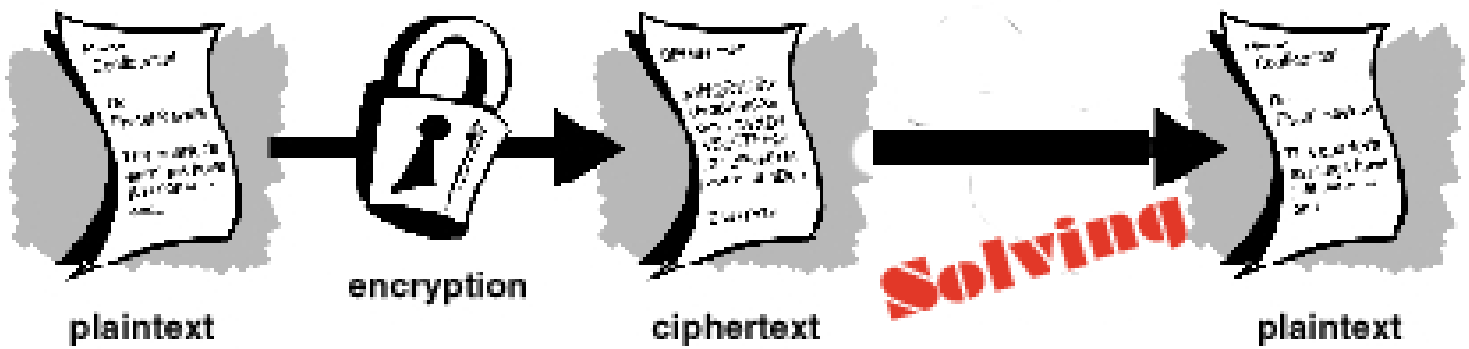
Algorithmes

- Complexité exponentielle en général
- Importance d'une bonne implantation
- Algorithmes $\mathrm{F4}$ et $\mathrm{F5}$



Applications

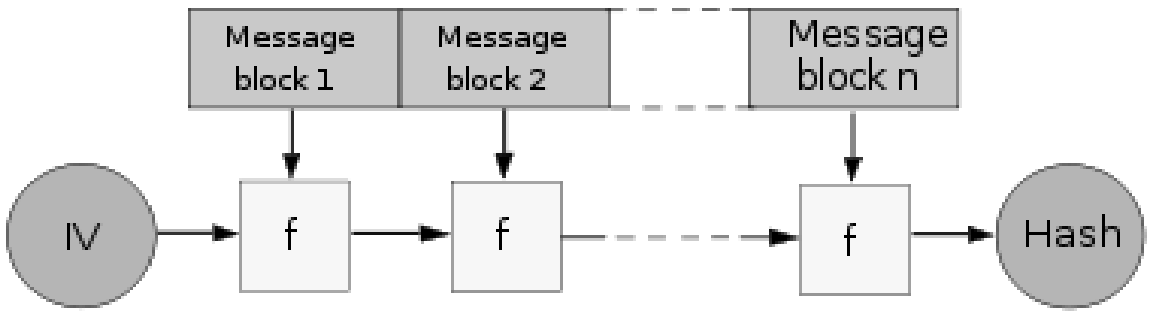
- Chiffrement par flot
- Chiffrement par blocs
- Fonctions de hachages
- Schémas multivariés



Fonctions de hachage

Fonction qui prend en entrée un message de longueur quelconque et produit en sortie une empreinte de longueur n :

$$h : \{0,1\}^* \rightarrow \{0,1\}^n$$



- Assurer l'intégrité d'un message
- Protection de mots de passe
- Signature électronique
- Génération pseudo-aléatoire

SHA-1

Opérations utilisées

- Opérations booléennes $(\wedge, \vee, \oplus)$
- Additions modulo 2^{32} (mots machine)

$f : \mathbb{F}_2^{160} \times \mathbb{F}_2^{512} \longrightarrow \mathbb{F}_2^{160}$

pour $i \in \{16, \ldots, 80\}$:

$m_i = (m_{i-3} \oplus m_{i-8} \oplus m_{i-14} \oplus m_{i-16})$

pour $i \in \{1, \ldots, 80\}$:

$a_i = (a_{i-1} \lll 5) + f_i(b_{i-1}, c_{i-1}, d_{i-1}) + e_{i-1} + m_i + k_i$

$b_i = a_{i-1}$

$c_i = (b_{i-1} \lll 30)$

$d_i = c_{i-1}$

$e_i = d_{i-1}$

fonction f_i :

$$\begin{aligned} \text{IF} &: (x \wedge y) \vee (\neg x \wedge z) \\ \text{XOR} &: x \oplus y \oplus z \\ \text{MAJ} &: (x \wedge y) \vee (x \wedge z) \vee (y \wedge z) \end{aligned}$$

Résultats

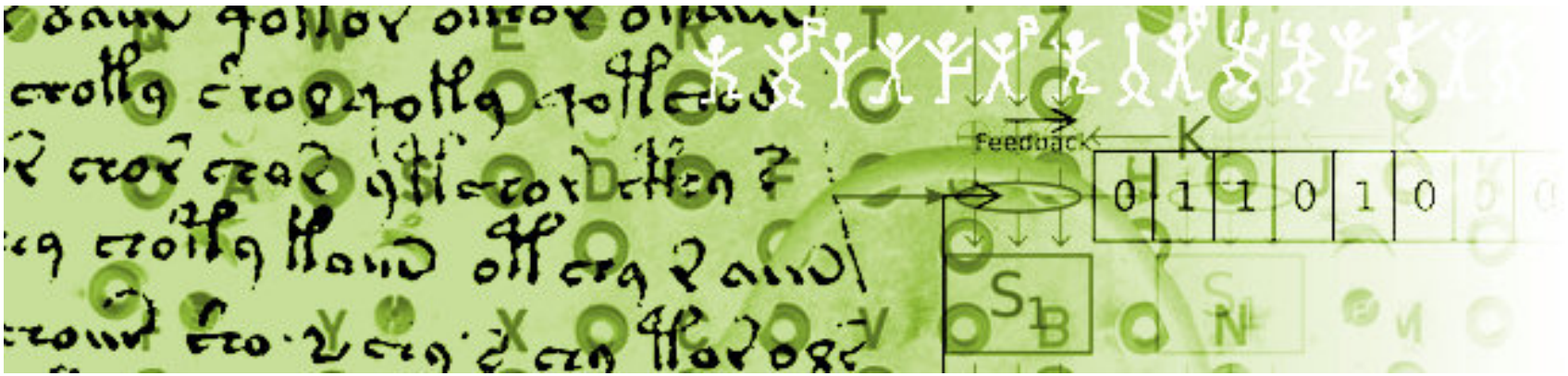
- Plate-forme logicielle pour attaques algébriques sur SHA-1 (Magma)
- Analyse de sécurité de fonctions de hachage multivariées

Attaque en collision sur les fonctions de hachage multivariées

$\#\mathbb{K}$	n	$n-k$	k	T_{F_5}	$\mathrm{Nop}_{\mathrm{F}_5}$	N	$\mathrm{N}_{\mathrm{gen}}$
2^{16}	16	15	1	≈ 1 h.	$2^{36.9}$	$2^{52.9}$	2^{128}
		14	2	126 s.	$2^{32.3}$	$2^{64.3}$	
2^{8}	20	18	2	51 h.	2^{41}	2^{57}	2^{80}
		17	3	2h45min.	2^{37}	2^{61}	
		16	4	643.1 s.	2^{34}	2^{66}	

FIG.: Temps de résolution et complexité

Travaux en cours



- Cryptanalyse systématique d'autres schémas
- Attaques en préimage sur SHA-1
- Bornes précises pour les schémas multivariés