Cryptanalyse des chiffrements GEA-1 et GEA-2 (GPRS)

Backdoor, Régulation et Propriété

Yann Rotella

Université de Versailles Saint Quentin en Yvelines

Février 2022

Histoire

1982 GSM (Global System for Mobile communications - 2G), A5/1 and A5/2

2000 GPRS (General Packet Radio Service), GEA-1 and GEA-2

A5/1 et A5/2

- Chiffrement à flot, clef de 64 bits

94 - 1999 Spécification rendue publique

1997 Golic, 2^{40}

1999 Goldberg, Wagner, attaque pratique sur A5/2

2000 Biryukov, Shamir et Wagner, compromis temps mémoire : temps réel, mais 2^{48}

2003 Ekdahl et Johannson, quelques minutes

2006 GSMA stoppe l'implémentation de A5/2

KASUMI,

Export Restrictions

ETSI (1998)

- ”the algorithm should be generally exportable taking into account current export restrictions”
- ”within this operational context, the algorithm provides an adequate level of security against eavesdropping of GSM GPRS services”

Restrictions ?

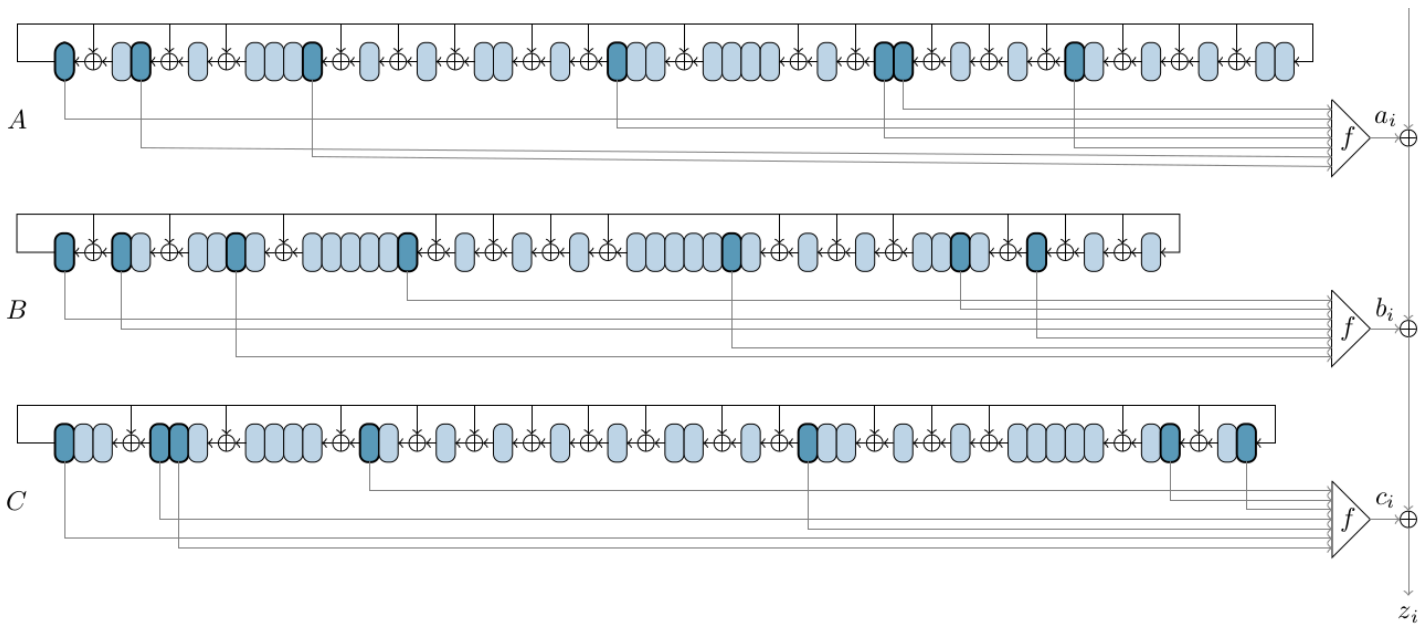
- http ://www.cryptolaw.org/
- France ?

GEA-1 et GEA-2 avant notre travail

- Propriétaire, chiffrement à flot
- designed by Security Algorithms Group of Experts (ETSI) in 1998
- ETSI interdit l'implémentation de GEA-1 en 2013
- GEA-2 encore obligatoire
- aucune divulgation ou analyse publique

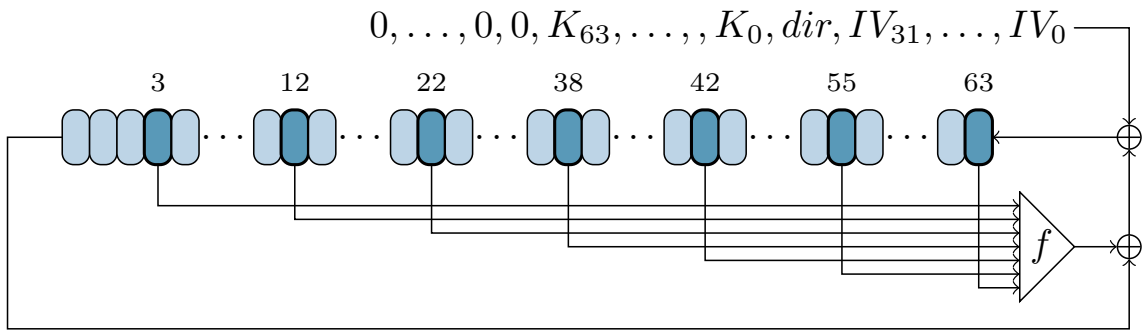
GEA-1

- clef de 64 bits introduite linéairement dans un registre de 96 bits
- 1600 octets de suite chiffrante (z_i), puis session suivante.



INITIALISATION

S, 225 fois :



Puis, 64 fois :

- $A \leftarrow s_0 s_1 \cdots s_{63}$
- $B \leftarrow s_{16} s_{17} \cdots s_{15}$
- $C \leftarrow s_{32} s_{33} \cdots s_{31}$

FAIBLESSE DE L'INITIALISATION

La relation entre S et A, B et C est linéaire, on peut donc construire $M_A \in \mathcal{M}(31 \times 64)$, $M_B \in \mathcal{M}(32 \times 64)$ et $M_C \in \mathcal{M}(33 \times 64)$.

FAIBLESSE DE L'INITIALISATION

La relation entre S et A, B et C est linéaire, on peut donc construire $M_A \in \mathcal{M}(31 \times 64)$, $M_B \in \mathcal{M}(32 \times 64)$ et $M_C \in \mathcal{M}(33 \times 64)$. Il s'avère que :

$$\dim(\ker(M_A) \cap \ker(M_C)) = 24$$

Une idée pour exploiter cela ?

FAIBLESSE DE L'INITIALISATION

La relation entre S et A, B et C est linéaire, on peut donc construire $M_A \in \mathcal{M}(31 \times 64)$, $M_B \in \mathcal{M}(32 \times 64)$ et $M_C \in \mathcal{M}(33 \times 64)$. Il s'avère que :

$$\dim(\ker(M_A) \cap \ker(M_C)) = 24$$

Une idée pour exploiter cela ? Donc,
$\mathbb{F}_2^{64} = \ker(M_B) \oplus (\ker(M_A) \cap \ker(M_C)) \oplus V$, $s = u + t + v$: précalcul : 2^{32}, online : 2^{40}

Par chance ou faiblesse intentionnelle ?

Quelle est la probabilité ?

Par chance ou faiblesse intentionnelle ?

Quelle est la probabilité ? LFSRs générés aléatoirement de tailles 31 et 33, avec une initialisation à la GEA-1 (10^6) :

intersection dim	< 6	6	7	8	9	10	11	12
# of spaces	998.027	1,490	366	86	26	5	0	0