Introduction à la cryptographie

Pierre-Alain Fouque
Université Rennes 1 et
Institut Universitaire de France (IUF)

Pierre-Alain.Fouque@ens.fr

Chiffrement par flot

Systèmes de chiffrement efficace en environnement très contraint (carte à puce GSM A5/1 par exemple)

Systèmes de chiffrement très efficace en logiciel (RC4 par exemple)

Construits à partir du chiffrement de Vernam qui garantit la sécurité parfaite

XOR

- XOR de deux chaînes binaires $\{0,1\}^n$, est l'addition modulo 2 bit à bit
- Table
- Bitwise : bit à bit
- Propriétés :
  - pour tout a, $a \oplus 0 = a$
  - pour tout a, $a \oplus 1 = 1\text{-}a$
  - pour tout a, $a \oplus a = 0$

Schémas symétriques

- Def: un chiffrement se définit par (K,M,C) est une paire d'algorithmes «efficaces» (E,D) où $E:K\times M\rightarrow C$, $D:K\times C\rightarrow M$ t.q. $\forall m\in M, k\in K, D(k,E(k,m))=m$
- E est souvent randomisé,
- D est toujours déterministe

One Time Pad
(Vernam 1917)

- c:=E(k,m)=k⊕m
- D(k,c)=k⊕c
-

msg: 0110111
⊕ k: 1011001
CT:

- En effet, D(k,E(k,m))=D(k,k⊕m)=k⊕(k⊕m)
  =(k⊕k)⊕m=0⊕m=m
- Etant donné un message (m) et son chiffrement OTP (c), pouvez-vous calculer la clé OTP à partir de m et c ?

One Time Pad (Vernam 1917)

- chiffrement et déchiffrement très très rapide !!
- .... mais clés très longues (aussi longue que le clair)
- Est-ce que le OTP est un bon chiffrement ?
- Qu'est-ce qu'un bon chiffrement ?

Stream cipher
(rendre OTP pratique)

- idée: remplacer la clé «aléatoire» par «pseudoaléa»
- PRG: est une fonction $G:\{0,1\}^s \rightarrow \{0,1\}^n$, $n>>s$

- (calculable «efficacement» par algo. déterministe)
- $c:=E(k,m):=m \oplus G(k)$
- $D(k,m)=c \oplus G(k)$
- Est-ce qu'un stream cipher garantit la sécurité parfaite ?

Générateurs pseudo-aléatoires

- Def: G algorithme déterministe en temps polynomial.

  Pour tout n, $s \in \{0,1\}^n$, le résultat de G(s) est une chaîne de bits

  de longueur m(n)

  - Expansion: m(n)>n, avec m un polynôme
  - Pseudo-aléatoire: Pour tout algorithme PPT (probabilistic polynomial-time) D, il existe une fonction négligeable negl: |Pr[D(G(s))=1]-Pr[D(r)=1]|<=negl(n) où s et r sont aléatoires et uniformes de la bonne taille

- Def: PRG est imprédictible s'il n'est pas prédictible
- ⇒∀i: aucun PPT. adv prédit bit (i+1) pour «non-negl» ε
- PRG faibles (ne pas les utiliser pour la crypto)
  - générateurs linéaires congruentiels parameètres a, b, p
  - r[0]≡seed, r[i]←ar[i-1]+b mod p, output bits of r[i]
  - glibc: random(): r[i]←(r[i-1]+ r[i-31]) $\%2^{32}$, output r[i]>>1
    - NE JAMAIS L'UTILISER EN CRYPTO !!!!

Attaques Stream cipher

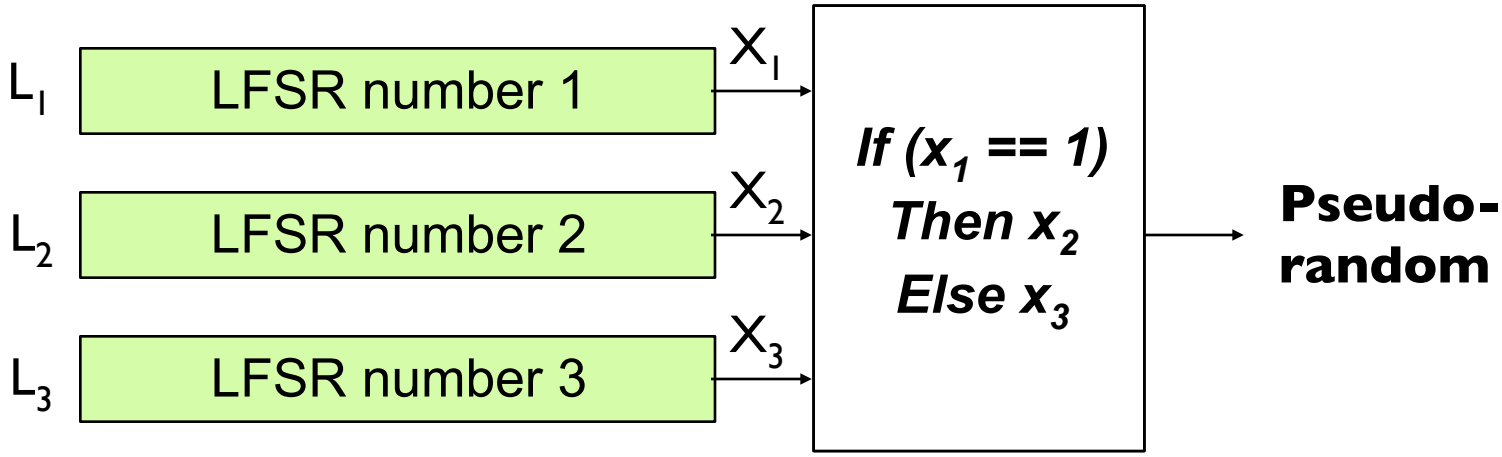
- Attack 1: two time pad n'est pas sûr
  - Jamais utiliser un stream cipher plus d'une fois !!
  - Exemples du monde réel
    - Project Venona (1941-1946)
    - MS-PPTP (Windows NT)
    - WEP-RC4 (802.11b)

Attaque Stream cipher

- Attack 2: aucune intégrité (OTP est malléable)

Modification de CT: indétectable et a un impact prédictible sur le clair PT

Geffe stream cipher



Quel est le biais ?