

One-Time Pad et Stream Cipher

Pierre-Alain Fouque

pa.fouque@gmail.com

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** (one-time pad=masque jetable) qui garantit la sécurité parfaite

Schémas symétriques

- Def: un chiffrement défini sur 3 espaces (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 **probabiliste**,
- D est toujours **déterministe**

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 , $a \oplus 1 = 1 - a$
 - pour tout a , $a \oplus a = 0$

One Time Pad (Vernam 1917)

- $c := E(k, m) = k \oplus m$
- $D(k, c) = k \oplus c$
- | | |
|---------------------|-----|
| msg: 0110111 | |
| $\oplus$ k: 1011001 | |
| | CT: |
- En effet, $D(k, E(k, m)) = D(k, k \oplus m) = k \oplus (k \oplus m) = (k \oplus k) \oplus m = 0 \oplus m = m$
- 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 ?

Sécurité au sens de la théorie de l'information (Shannon 1949)

- Idée de base: CT ne doit révéler aucune info sur PT
- Def: un chiffrement (E,D) sur (K,M,C) garantit la sécurité parfaite (inconditionnelle) if
 - $\forall m_0, m_1 \in M, (|m_0|=|m_1|)$ et $\forall c \in C, \Pr[E(k,m_0)=c] = \Pr[E(k,m_1)=c]$ où $k \leftarrow_R K$
 - Etant donné CT, on ne peut pas dire si le message est m_0 ou m_1 (pour tout m_0 et m_1)
 - Même les adversaires les plus puissants n'apprennent rien sur PT connaissant CT (aucune à chiffré seul connu CT, mais d'autres ...)

Lemme: OTP garantit la sécurité parfaite

- Preuve: $\forall m, c: \Pr_k[E(k, m) = c] = \frac{\# \text{ keys } k \in K \text{ s.t. } E(k, m) = c}{|K|}$
- donc, $\forall m, c, \#\{k \in K: E(k, m) = c\} = \text{const}$
- $\Rightarrow$ chiffrement garantit la sécurité parfaite
- Soient $m \in M$ et $c \in C$, combien de clé OTP envoie m vers c ?
- OTP garantit la sécurité parfaite

Propriété principale du XOR

- Thm: si Y est une variable aléatoire sur $\{0,1\}^n$, X une variable **uniforme et indépendante** sur $\{0,1\}^n$, alors $Z=Y\oplus X$ est une variable **uniforme** sur $\{0,1\}^n$
- Preuve:

Stream cipher

(rendre OTP pratique)

- idée: remplacer la clé «aléatoire» par «pseudoaléa»
- PRG: est une fonction $G:\{0,1\}^s \rightarrow \{0,1\}^n, n \gg s$
- (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 : $|\Pr[D(G(s))=1] - \Pr[D(r)=1]| \leq \text{negl}(n)$ où s et r sont aléatoires et uniformes de la bonne taille

Attaques Stream cipher

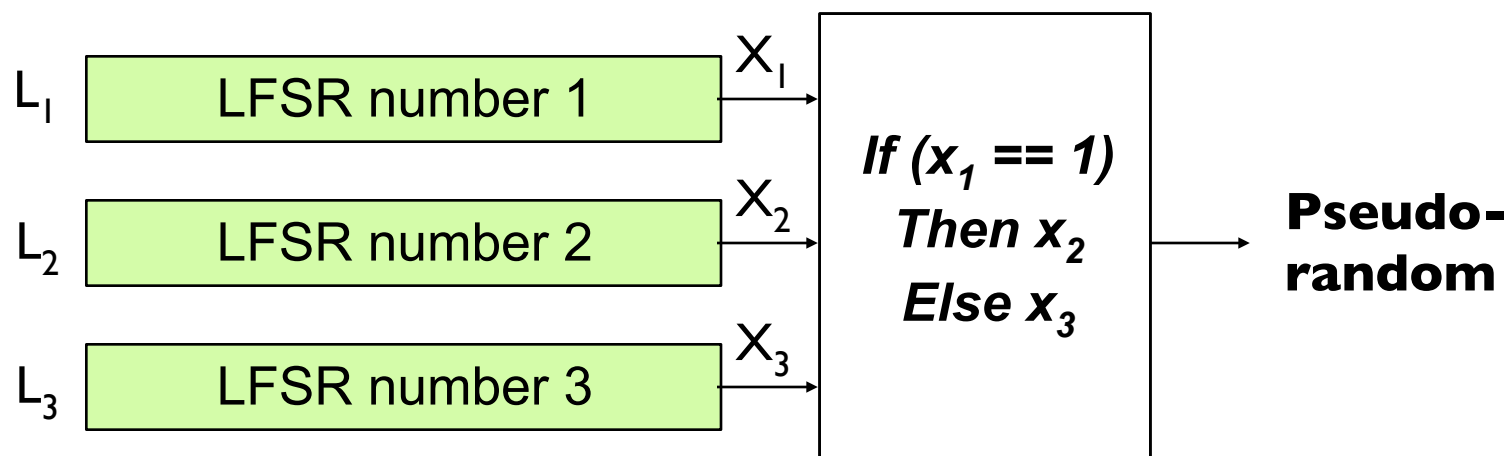
- Attack 1: two time pad n'est pas sûr
 - Jamais utiliser un stream cipher plus d'une fois !!
 - Exemples du monde réel
 - Project Venona (1941-1946)
 - MS-PPTP (Windows NT)
 - WEP-RC4 (802.11b)

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* ?