Analyse des cryptanalyses statistiques

Benoît Gérard

Séminaire « Protection de l'information »

-

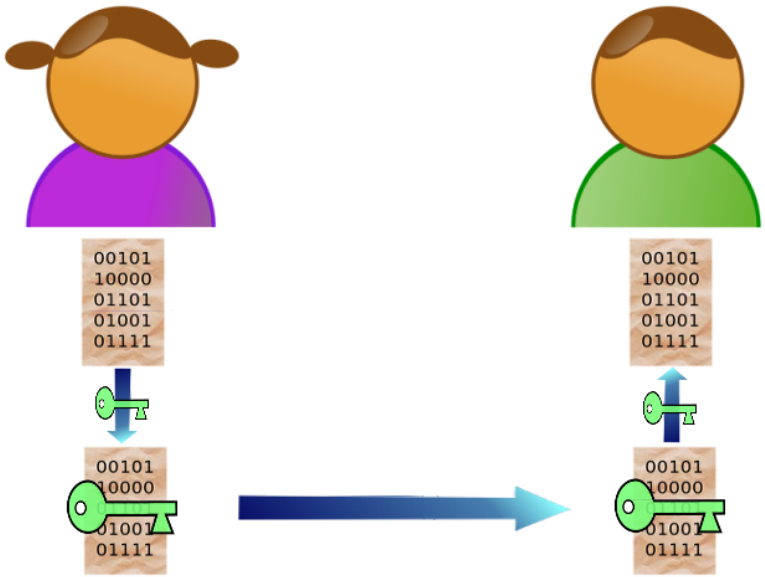
16 décembre 2010

Plan

Plan

Chiffrement symétrique / asymétrique (1/2)

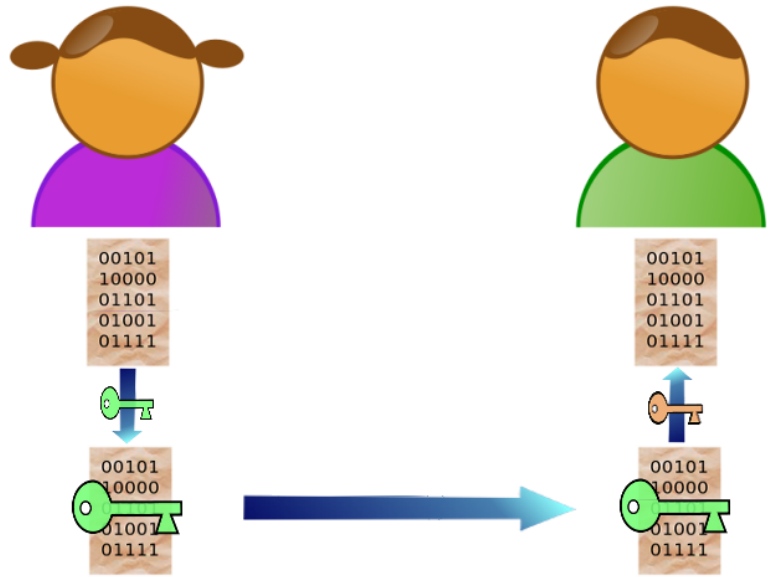
Symétrique



✓ Efficace.

x Pas de preuves de sécurité.

Asymétrique

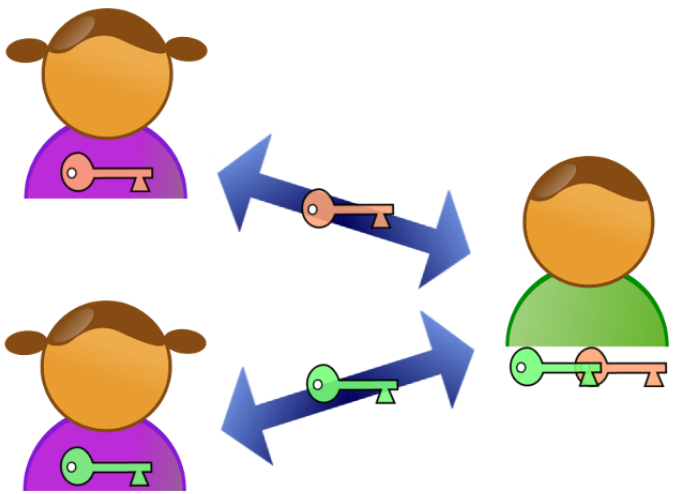


x Lent.

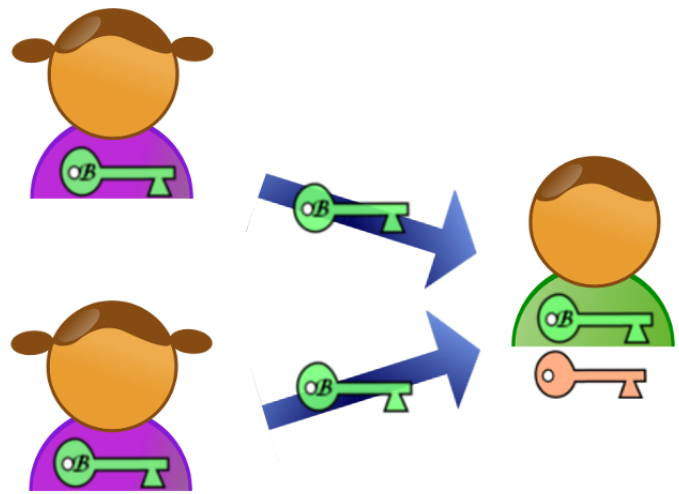
✓ Sécurité *prouvée*.

Chiffrement symétrique / asymétrique (2/2)

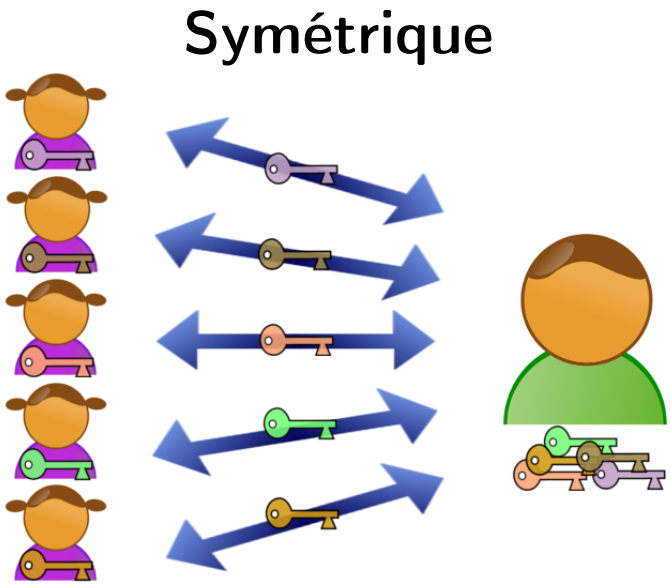
Symétrique

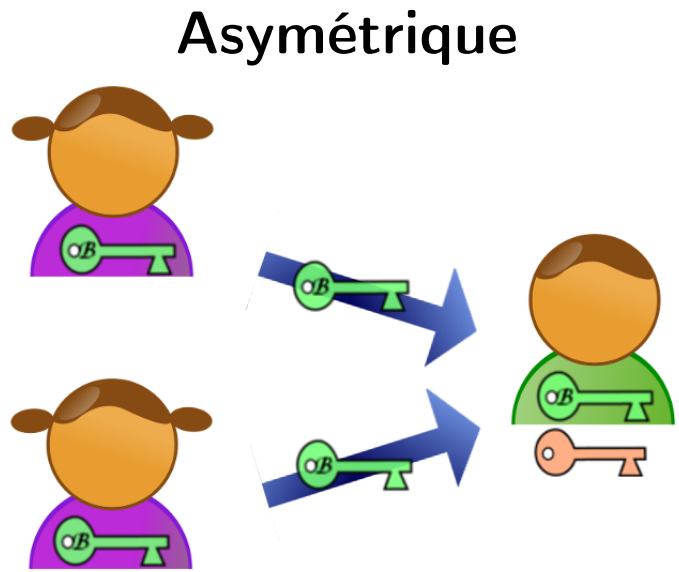


Asymétrique



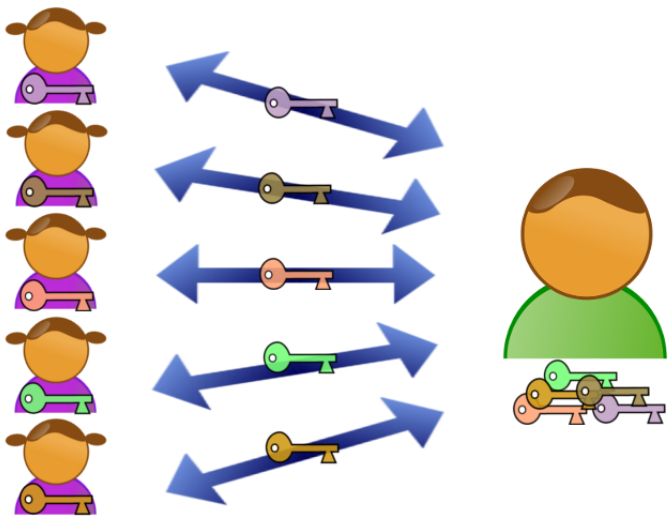
Chiffrement symétrique / asymétrique (2/2)



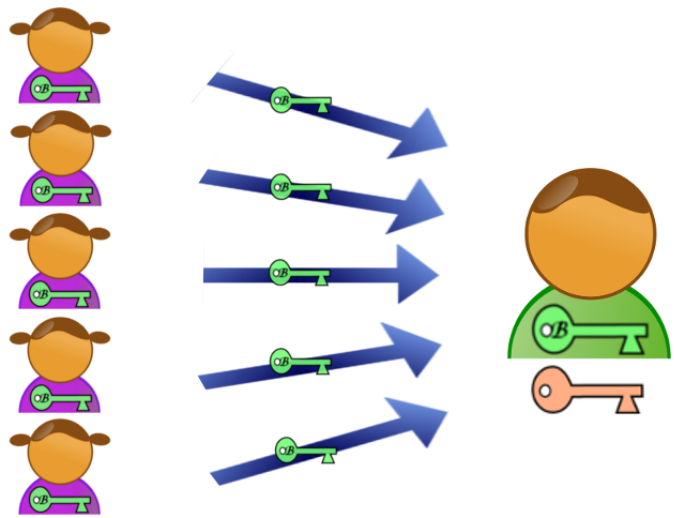


Chiffrement symétrique / asymétrique (2/2)

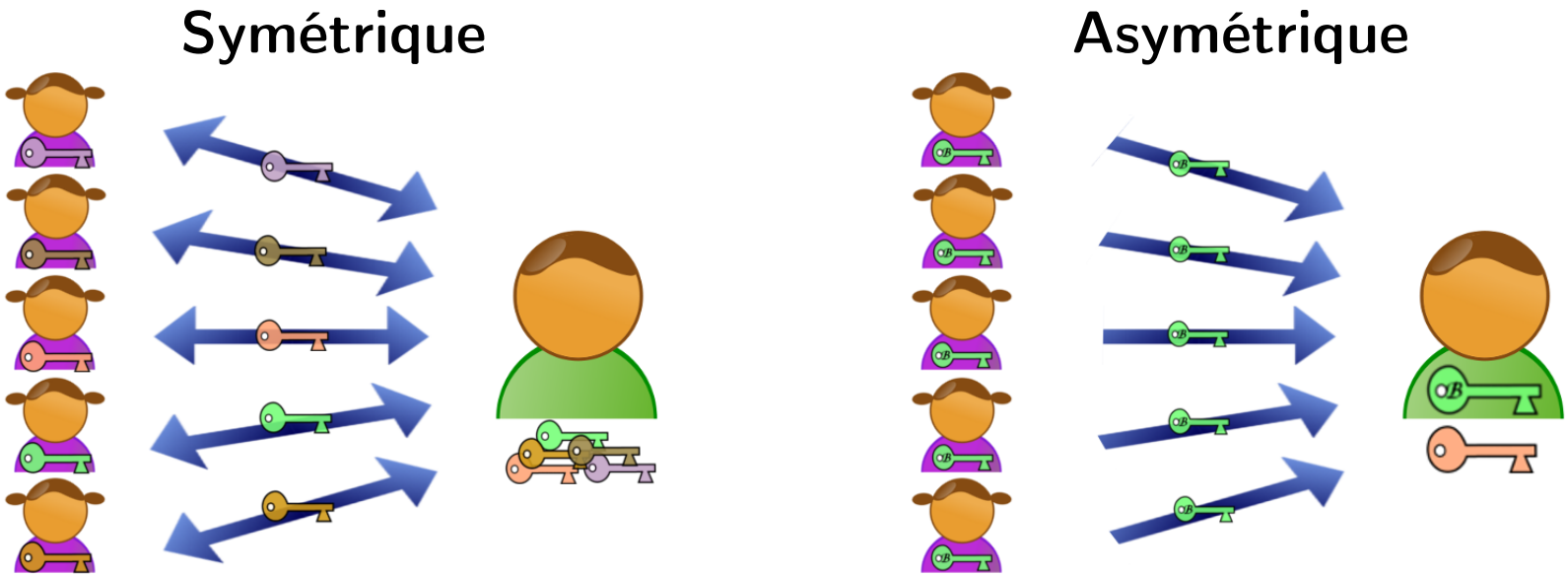
Symétrique



Asymétrique



Chiffrement symétrique / asymétrique (2/2)

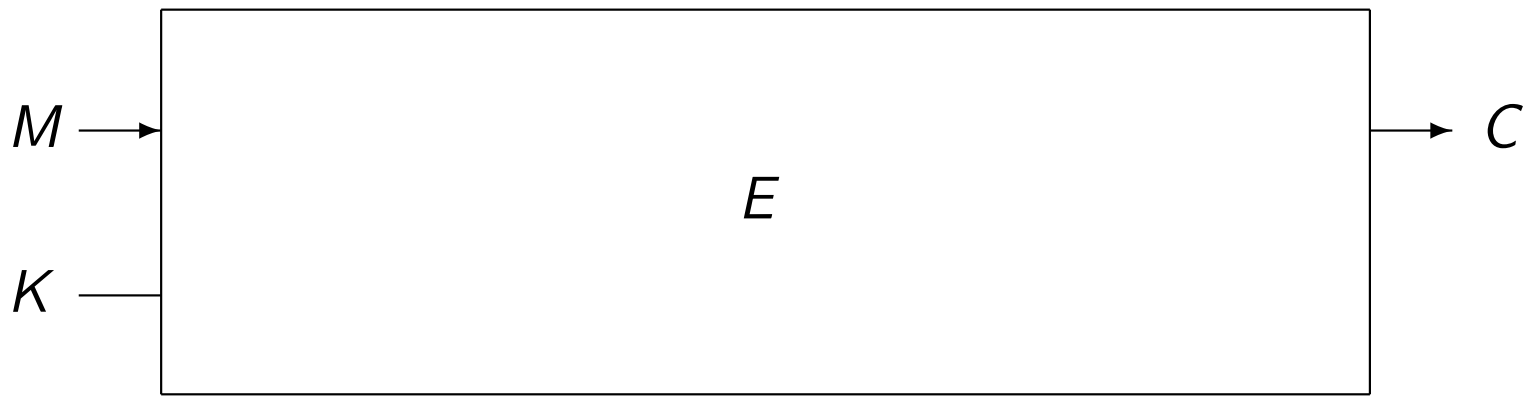


Systèmes hybrides :

- Échange de clef : algorithme asymétrique.
- Chiffrement du message : algorithme symétrique.

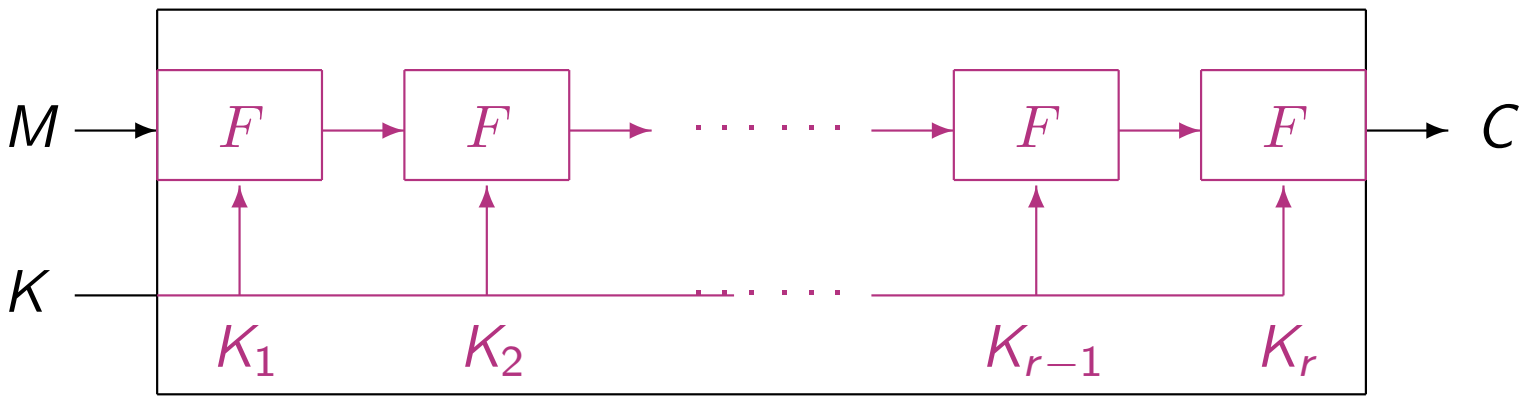
Chiffrement itératif par bloc

Les chiffrements symétriques par bloc sont la cible privilégiée des cryptanalyses statistiques.



Chiffrement itératif par bloc

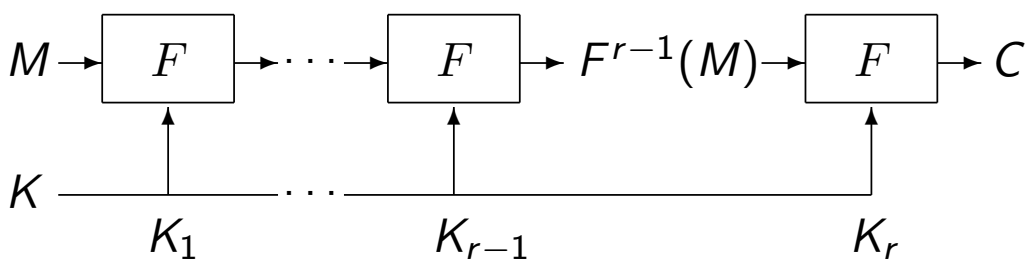
Les chiffrements symétriques par bloc sont la cible privilégiée des cryptanalyses statistiques.



Plan

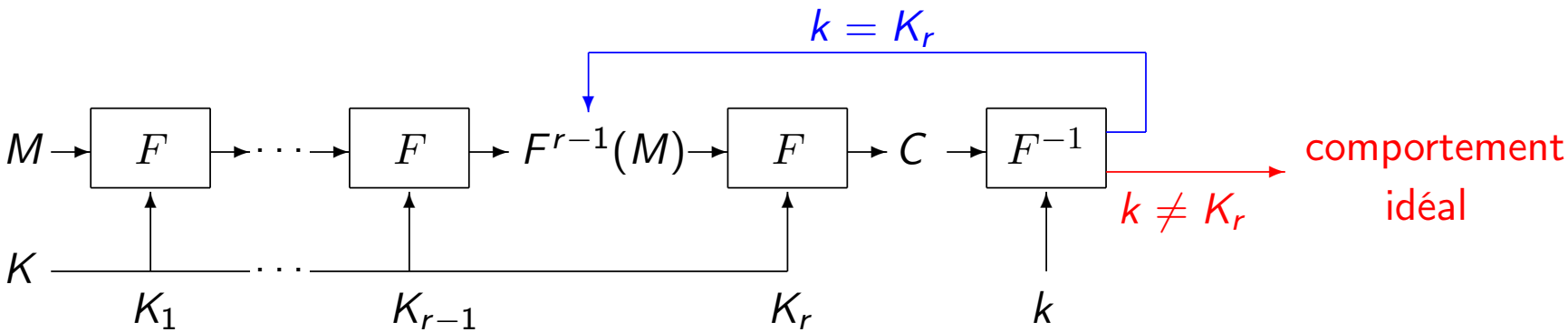
Exemple typique : attaque sur le dernier tour

1. Trouver une caractéristique statistique sur les $r-1$ premiers tours (un phénomène non-idéal).



Exemple typique : attaque sur le dernier tour

1. Trouver une caractéristique statistique sur les $r-1$ premiers tours (un phénomène non-idéal).
2. Pour chaque candidat k pour K_r
   - Appliquer F^{-1} avec k aux chiffrés.
   - Générer le compteur correspondant.
3. Trier les candidats par vraisemblance.
4. Tester les clefs maîtres correspondant au candidat le plus vraisemblable, puis au second, ...



Choix d'une caractéristique statistique

Problématiques

- x Il y a un nombre trop important de caractéristiques.
- x Calculer leur probabilité demande de chiffrer tous les messages avec toutes les clefs.
- x On calcule, a priori, la probabilité moyenne sur les clefs.

Solutions

- Chercher uniquement les meilleures caractéristiques.
- Calculer la probabilité sur un tour puis « chaîner » en supposant les tours indépendants.
- Supposer que cette probabilité ne dépend pas de la clef utilisée.

Hypothèses principales

Lors de l'analyse d'une cryptanalyse statistique, on effectue souvent trois hypothèses.

- Hypothèse de répartition aléatoire par fausse clef.
- Hypothèse d'indépendance des tours.
- Hypothèse d'équivalence stochastique (clef fixée).

Hypothèses principales

Lors de l'analyse d'une cryptanalyse statistique, on effectue souvent trois hypothèses.

- Hypothèse de répartition aléatoire par fausse clef.
- Hypothèse d'indépendance des tours.
- Hypothèse d'équivalence stochastique (clef fixée).

Comportement des mauvais compteurs

Si la sortie de $r+1$ tours du chiffrement n'est pas idéale, alors on peut attaquer $r+2$ tours du chiffrement plutôt que r.

Attention toutefois aux cryptanalyses multiples !

Hypothèses principales

Lors de l'analyse d'une cryptanalyse statistique, on effectue souvent trois hypothèses.

- Hypothèse de répartition aléatoire par fausse clef.
- Hypothèse d'indépendance des tours.
- Hypothèse d'équivalence stochastique (clef fixée).

Pour les cas particuliers

- cryptanalyse différentielle ;
- cryptanalyse linéaire.

Plan

Présentation

- Caractéristique statistique : différentielle $(\delta_1, \delta_2) \in \mathbb{F}_2^s \times \mathbb{F}_2^s$

$$\Pr_{M,K}\left[F_K^{r-1}(M) \oplus F_K^{r-1}(M \oplus \delta_1) = \delta_2\right] = p_{\delta_1 \to \delta_2}.$$

- Les N échantillons sont $(m_1^i, m_2^i, c_1^i, c_2^i)$ où $m_1^i \oplus m_2^i = \delta_1$ et les c^i sont les chiffrés correspondant.

$$\Sigma_k^i = \begin{cases} 1 & \text{si } F_k^{-1}(c_1^i) \oplus F_k^{-1}(c_2^i) = \delta_2 \\ 0 & \text{sinon.} \end{cases}$$

$$\Sigma_k = \sum_{i=1}^{N} \Sigma_k^i.$$

- On s'attend à

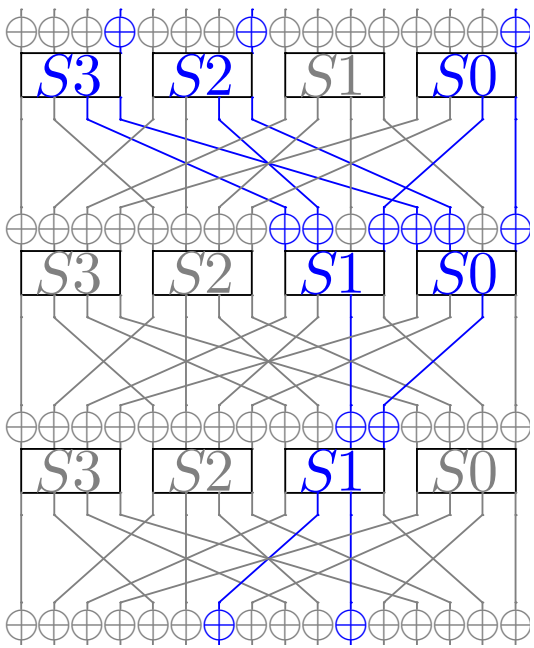
$$\Sigma_{k=k^*} \sim \mathcal{B}in\left(N, p_{\delta_1 \to \delta_2}\right) \quad \text{et} \quad \Sigma_{k \neq k^*} \sim \mathcal{B}in\left(N, 2^{-s}\right).$$

Estimer la probabilité d'une différentielle

Chemin différentiel

Un chemin différentiel : $\beta = (\beta_0, \ldots, \beta_r) \in \mathbb{F}_2^s \times \cdots \times \mathbb{F}_2^s$.

$$p_\beta \stackrel{\text{def}}{=} \Pr_{M,K}\left[\forall\, i\,, F_K^i(M) \oplus F_K^i(M \oplus \beta_0) = \beta_i\right].$$



$$\begin{aligned}\beta_0 &= \texttt{0x1101},\\ \beta_1 &= \texttt{0x00BB},\\ \beta_2 &= \texttt{0x0030},\\ \beta_3 &= \texttt{0x0220}.\end{aligned}$$

Estimer la probabilité d'une différentielle

Probabilité d'une différentielle

$$p_{\delta_1 \to \delta_2} = \sum_{\beta=(\delta_1,\beta_1,\ldots,\beta_{r-1},\delta_2)} p_\beta.$$

Difficulté : calculer les probabilités de tous les chemins.

Dans la littérature, on utilise des bornes inférieures :

- ✗ Regarder le chemin le plus probable.
- ✓ Regarder le plus de chemins possible.

Probabilité à clef fixée

Chiffrement de Markov et chaînage

Définition : Chiffrement de Markov

Un chiffrement itératif est dit de Markov si pour une distribution uniforme de la sous-clef K, on a, pour tout $x \in \mathbb{F}_2^s$,

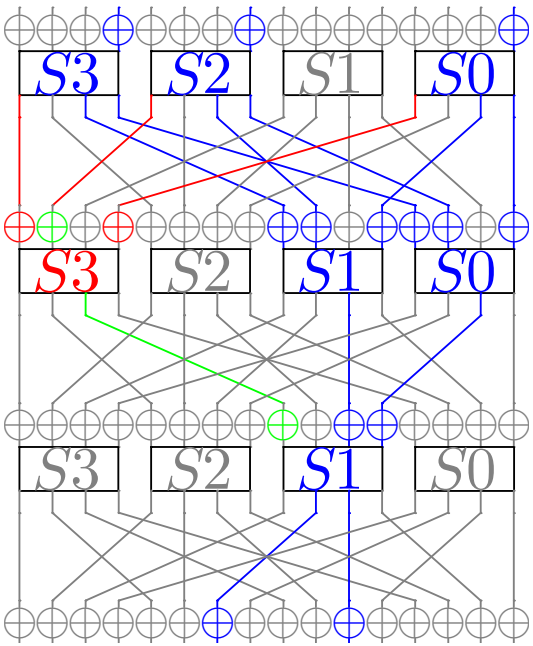
$$\Pr_{K,X}\left[F_K(X) \oplus F_K(X \oplus \delta_1) = \delta_2 | X = x\right] = \Pr_{K,X}\left[F_K(X) \oplus F_K(X \oplus \delta_1) = \delta_2\right].$$

Alors, si les valeurs intermédiaires du chiffrement sont uniformément distribuées,

$$p_\beta = \prod_{i=1}^{r} \Pr_{K,X}\left[F_K(X) \oplus F_K(X \oplus \beta_{i-1}) = \beta_i\right].$$

Probabilité à clef fixée

Indépendance des tours



- 0x1 $\longrightarrow$0x3 implique 0.
- 0x3 $\longrightarrow$0x6 implique 1.
- Les deux bits de clef verts correspondent au même bit de clef maître.

Bits de clef	000	001	010	011
Probabilité du 1	1/2	1/2	1/2	1
Bits de clef	100	101	110	111
Probabilité du 1	1	1/2	1	0

Probabilité à clef fixée

Chaînage et probabilité globale

Le produit des probabilités de transition donne une bonne idée de la probabilité

$$\Pr_{X,K}\left[\forall\, i\,, F_K^i(X) \oplus F_K^i(X \oplus \beta_{i-1}) = \beta_i\right],$$

qui peut être différente de la probabilité à clef fixée k^*

$$\Pr_{X,K}\left[\forall\, i\,, F_K^i(X) \oplus F_K^i(X \oplus \beta_{i-1}) = \beta_i | K = k^*\right].$$

Probabilité à clef fixée

Distribution de la probabilité à clef fixée 1/2

[Daemen et Rijmen 2007] : *sampling model*.

- On regarde des boules blanches représentant les couples (m, k).
- On peint en noir les boules telles que

$$E_k(m) \oplus E_k(m \oplus \delta_1) = \delta_2.$$

- On a $2^{s-1} \cdot 2^{n_{key}} \cdot p_{\delta_1 \to \delta_2}$ boules noires.

Modèle Sampling model

Fixer une clef revient à tirer aléatoirement 2^{s-1} boules.

La probabilité à clef fixée suit donc une loi hypergéométrique.

Probabilité à clef fixée

Distribution de la probabilité à clef fixée 2/2

$$\Pr\left[\Pr_M\left[E_{k^*}(M) \oplus E_{k^*}(M \oplus \delta_1) = \delta_2\right] = i \cdot 2^{1-s}\right]$$

$$=$$

$$\binom{p_{\delta_1 \to \delta_2}\, 2^{n_{key}+s-1}}{i} \binom{(1-p_{\delta_1 \to \delta_2})\, 2^{n_{key}+s-1}}{2^{s-1} i} \binom{2^{n_{key}+s-1}}{2^{s-1}}^{-1}$$

$$\approx$$

$$\binom{2^{s-1}}{i} p_{\delta_1 \to \delta_2}^{i} (1-p_{\delta_1 \to \delta_2})^{2^{s-1}-i}.$$

Plan

Présentation

- Caractéristique statistique : approximation linéaire

$$\Pr_{M,K}\left[\pi \cdot M \oplus \gamma \cdot F_K^{r-1}(M) = 0\right] = \frac{1}{2} + \varepsilon.$$

- On regarde le compteur extrait des N couples (m^i, c^i) :

$$\Sigma_k = \sum_{i=1}^{N} \pi \cdot m^i \oplus \gamma \cdot F_k^{-1}(c^i).$$

- On s'attend à

$$\Sigma_{k=k^*} \sim \mathcal{B}in\left(N, \frac{1}{2} - (-1)^{\kappa \cdot K}\varepsilon\right) \quad \text{et} \quad \Sigma_{k\neq k^*} \sim \mathcal{B}in\left(N, \frac{1}{2}\right).$$

Trouver des approximations linéaires

Chaînage

On peut utiliser :

- décodage du Reed-Muller d'ordre 1 ;
- chaînage.

On chaîne des approximations sur un tour :

$$\Pr_{M_0,K_0}[\omega_0 \cdot M_0 \oplus \omega_1 \cdot F_{K_0}(M_0) = 0] = \frac{1}{2} + \varepsilon_1,$$

$$\Pr_{M_1,K_1}[\omega_1 \cdot M_1 \oplus \omega_2 \cdot F_{K_1}(M_1) = 0] = \frac{1}{2} + \varepsilon_2,$$

pour obtenir

$$\Pr_{M_0,(K_0,K_1)}[\omega_0 \cdot M_0 \oplus \omega_2 \cdot F_{K_1} \circ F_{K_0}(M_0) = 0] = \frac{1}{2} + 2\varepsilon_1\varepsilon_2.$$

Trouver des approximations linéaires

Masque de clef

Dans les chiffrements dits « alternants » où la clef est combinée à l'état par une addition modulo 2, on obtient un masque de clef κ.

$$\Pr_{M,K}\left[\pi \cdot M \oplus \gamma \cdot E_K(M) = \kappa \cdot K\right] = \frac{1}{2} + \varepsilon.$$

En effet, on peut écrire $F_K(M) = F_0(M \oplus K)$. On réécrit alors

$$\Pr_{M_0,K_0}\left[\omega_0 \cdot M_0 \oplus \omega_1 \cdot F_{K_0}(M_0) = 0\right] = \frac{1}{2} + \varepsilon_1$$

en

$$\Pr_{M'_0,K_0}\left[\omega_0 \cdot (M'_0 \oplus K_0) \oplus \omega_1 \cdot F_0(M'_0) = 0\right] = \frac{1}{2} + \varepsilon_1.$$

Trouver des approximations linéaires

Masque de clef : précisions

Pour être précis, on obtient des masques de clef pour chaque tour :

$$\kappa_1, \ldots, \kappa_r.$$

Et donc on peut écrire

$$\Pr_{M,K}\left[\pi \cdot M \oplus \gamma \cdot E_K(M) = \bigoplus_{i=1}^{r} \kappa_i \cdot K_i\right] = \frac{1}{2} + \varepsilon.$$

Dans le cas particulier où l'algorithme de cadencement de clef est linéaire, on peut alors calculer κ tel que

$$\Pr_{M,K}\left[\pi \cdot M \oplus \gamma \cdot E_K(M) = \kappa \cdot K\right] = \frac{1}{2} + \varepsilon.$$

Problème à clef fixée

Présentation du problème

Pour une approximation (π, γ, κ) de biais ε, on peut écrire

$$\Pr_{M,K}\left[\pi \cdot M \oplus \gamma \cdot E_K(M) = 0\right] = \frac{1}{2} + (-1)^{\kappa \cdot K}\varepsilon.$$

Supposons que l'on ait deux approximations

$$\begin{aligned}\Pr_{M,K}\left[\pi \cdot M \oplus \gamma \cdot E_K(M) = 0\right] &= \frac{1}{2} + (-1)^{\kappa \cdot K}\,\varepsilon,\\ \Pr_{M,K}\left[\pi \cdot M \oplus \gamma \cdot E_K(M) = 0\right] &= \frac{1}{2} + (-1)^{\kappa' \cdot K}\,\varepsilon',\end{aligned}$$

avec $\varepsilon \neq \varepsilon'$.

Que vaut $\Pr_{M,K}\left[\pi \cdot M \oplus \gamma \cdot E_K(M) = 0 | K = k^*\right]$?

Problème à clef fixée

Cryptanalyse linéaire et fonctions booléennes

Pour des masques (π, γ) donnés, on considère la fonction booléenne

$$g_{k^*} : m \mapsto \pi \cdot m \oplus \gamma \cdot E_{k^*}(m).$$

On va s'intéresser aux corrélations de fonctions booléennes.

Définition

Soient g_1 et g_2 deux fonctions booléennes définies sur $\mathbb{F}_2^n$, on définit

$$c(g_1, g_2) \stackrel{\text{def}}{=} \frac{\#\{x, g_1(x) = g_2(x)\} - \#\{x, g_1(x) \neq g_2(x)\}}{2^n},$$

$$c(g_1) \stackrel{\text{def}}{=} c(g_1, 0) = \frac{\#\{x, g_1(x) = 0\} - \#\{x, g_1(x) = 1\}}{2^n}.$$

Problème à clef fixée

Objectif

On notera $c(\omega_{i-1} \cdot x \oplus \omega_i \cdot F_{k_i^*}(x))$ la corrélation de la fonction booléenne

$$x \mapsto \omega_{i-1} \cdot x \oplus \omega_i \cdot F_{k_i^*}(x).$$

On veut montrer que pour des sous-clefs $k_1^*, \ldots, k_r^*$ issues de k^*,

$$c(\pi \cdot m \oplus \gamma \cdot E_{k^*}(m)) = \sum_{\omega=(\pi,\omega_1,\ldots,\omega_{r-1},\gamma)} \prod_{i=1}^{r} c(\omega_{i-1} \cdot x \oplus \omega_i \cdot F_{k_i^*}(x)).$$

Chaînage : pour un chemin $\omega = (\omega_0, \ldots, \omega_r)$, on obtient $(\kappa_1, \ldots, \kappa_r, \varepsilon)$ tels que pour toute clef k^* et ses dérivées $(k_1^*, \ldots, k_r^*)$,

$$\begin{aligned} \prod_{i=1}^{r} c(\omega_{i-1} \cdot x \oplus \omega_i \cdot F_{k_i^*}(x)) &= (-1)^{\bigoplus_{i=1}^{r} \kappa_i \cdot k_i^*} \frac{\varepsilon}{2}, \\ &\stackrel{?}{=} (-1)^{\kappa \cdot k^*} \frac{\varepsilon}{2}. \end{aligned}$$

Problème à clef fixée

Objectif

On notera $c(\omega_{i-1} \cdot x \oplus \omega_i \cdot F_{k_i^*}(x))$ la corrélation de la fonction booléenne

$$x \mapsto \omega_{i-1} \cdot x \oplus \omega_i \cdot F_{k_i^*}(x).$$

On veut montrer que pour des sous-clefs $k_1^*, \ldots, k_r^*$ issues de k^*,

$$c(\pi \cdot m \oplus \gamma \cdot E_{k^*}(m)) = \sum_{\omega=(\pi,\omega_1,\ldots,\omega_{r-1},\gamma)} \prod_{i=1}^{r} c(\omega_{i-1} \cdot x \oplus \omega_i \cdot F_{k_i^*}(x)).$$

Chaînage : pour un chemin $\omega = (\omega_0, \ldots, \omega_r)$, on obtient $(\kappa_1(\omega), \ldots, \kappa_r(\omega), \varepsilon(\omega))$ tels que pour toute clef k^* et ses dérivées $(k_1^*, \ldots, k_r^*)$,

$$\begin{aligned} \prod_{i=1}^{r} c(\omega_{i-1} \cdot x \oplus \omega_i \cdot F_{k_i^*}(x)) &= (-1)^{\bigoplus_{i=1}^{r} \kappa_i(\omega) \cdot k_i^*} \frac{\varepsilon(\omega)}{2}, \\ &\stackrel{?}{=} (-1)^{\kappa(\omega) \cdot k^*} \frac{\varepsilon(\omega)}{2}. \end{aligned}$$

Problème à clef fixée

Pour deux tours 1/2

On veut montrer que, pour une clef k^* à laquelle correspondent les sous-clefs (k_1^*, k_2^*),

$$c(\pi \cdot m \oplus \gamma \cdot E_{k^*}(m)) = \sum_{\omega_1} c(\pi \cdot x \oplus \omega_1 \cdot F_{k_1^*}(x)) c(\omega_1 \cdot x \oplus \gamma \cdot F_{k_2^*}(x)).$$

$$\begin{aligned}
\textstyle\sum_{\omega_1} \quad & c(\pi \cdot x \oplus \omega_1 \cdot F_{k_1^*}(x)) c(\omega_1 \cdot x \oplus \gamma \cdot F_{k_2^*}(x)), \\
= \quad & \sum_{\omega_1} \left(2^{-n} \sum_{x} (-1)^{\pi \cdot x \oplus \omega_1 \cdot F_{k_1^*}(x)} \right) \left(2^{-n} \sum_{y} (-1)^{\omega_1 \cdot y \oplus \gamma \cdot F_{k_2^*}(y)} \right), \\
= \quad & 2^{-2n} \sum_{\omega_1} \sum_{x,y} (-1)^{\pi \cdot x \oplus \omega_1 \cdot \left[F_{k_1^*}(x) \oplus y \right] \oplus \gamma \cdot F_{k_2^*}(y)}, \\
= \quad & 2^{-2n} \sum_{\omega_1} \sum_{x,y} (-1)^{\pi \cdot x \oplus \gamma \cdot F_{k_2^*}(y)} (-1)^{\omega_1 \cdot \left[F_{k_1^*}(x) \oplus y \right]}.
\end{aligned}$$

Problème à clef fixée

Pour deux tours 2/2

$$
\begin{aligned}
\sum_{\omega_1} \quad & c(\pi \cdot x \oplus \omega_1 \cdot F_{k_1^*}(x)) c(\omega_1 \cdot x \oplus \gamma \cdot F_{k_2^*}(x)), \\
= \quad & 2^{-2n} \sum_{\omega_1, x, y} (-1)^{\pi \cdot x \oplus \gamma \cdot F_{k_2^*}(y)} (-1)^{\omega_1 \cdot \left[F_{k_1^*}(x) \oplus y \right]}, \\
= \quad & 2^{-n} \sum_{x} (-1)^{\pi \cdot x \oplus \gamma \cdot F_{k_2^*}(F_{k_1^*}(x))}, \\
= \quad & c(\pi \cdot m \oplus \gamma \cdot E_{k^*}(m)).
\end{aligned}
$$

On peut prouver la formule pour un nombre de tours quelconque par récurrence.

Plan

Différence **majeure** entre cryptanalyse linéaire et différentielle

Cryptanalyse différentielle

- ✗ Calcul de la probabilité d'un chemin en moyenne sur les clefs pas forcément exacte.
- ✗ Beaucoup de chemins à prendre en compte.

$$p_{\delta_1 \to \delta_2} = \sum_{\beta=(\delta_1,\beta_1,\ldots,\beta_{r-1},\delta_2)} p_\beta .$$

  - ✓ Atténue le premier point.
  - ✓ Sommer sur une partie des chemins donne une borne inférieure.
- ✗ Hypothèse d'équivalence à clef fixée fausse.
  - ✓ Sampling model : loi hypergéométrique.

Différence **majeure** entre cryptanalyse linéaire et différentielle

Cryptanalyse linéaire

- ✓ Le chaînage calcule précisément le biais moyen d'un chemin sur les clefs.
- x Beaucoup de chemins à prendre en compte pour une clef fixée :

$$\sum_{\omega=(\pi,\omega_1,\ldots,\omega_{r-1},\gamma)} (-1)^{\kappa(\omega)\cdot k^*} \frac{\varepsilon(\omega)}{2}.$$

  - x Sommer sur une petite partie des chemins ne donne aucune indication.