Indifférentiabilité et modèles de preuve idéalisés

Yannick Seurin

ANSSI, Laboratoire de cryptographie

21 février 2012

Univ. Limoges, Séminaire Crypto

Introduction

Principaux types de preuves de sécurité en cryptographie :

- preuves de sécurité inconditionnelles (sécurité au sens de la théorie de l'information) : valable contre des attaquants à capacité de calculs non bornée, schémas inefficaces (one-time pad)
- modèle standard : adversaires polynomiaux, repose sur des hypothèses de complexité non prouvées (factorisation, log discret)
- modèles idéalisés : modélisation parfaite de certaines primitives, moins fort que le modèle standard mais donne des schémas très efficaces

On va s'intéresser aux liens entre les deux principaux modèles idéalisés : ROM (*Random Oracle Model*) et ICM (*Ideal Cipher Model*)

Plan

1. Modèles de preuve idéalisés
2. Indifférentiabilité : définition
3. Attaque du schéma de Feistel à 5 tours
4. Indifférentiabilité du schéma de Feistel pour 14 tours
5. Indifférentiabilité publique et résistance à la corrélation

Plan

Modèle standard vs. modèles idéalisés

- deux primitives cryptographiques fondamentales :
  - fonction de hachage : $H : \{0,1\}^* \rightarrow \{0,1\}^n$, calculable efficacement
  - chiffrement par blocs : $E : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$, $E(K,\cdot)$ bijectif, efficacement calculable et inversible
- hypothèses de sécurité dans le modèle standard :
  - fonction de hachage : résistance à la pré-image, aux collisions, etc.
  - chiffrement par blocs : permutation pseudo-aléatoire
- souvent, ces hypothèse ne sont pas suffisantes pour prouver la sécurité d'un cryptosystème

  $\Rightarrow$ on a recours à des modèles idéalisés :
  - fonction de hachage : modèle de l'oracle aléatoire
  - chiffrement par blocs : modèle du chiffrement idéal

Fonctions de hachage, modèle standard

Propriétés attendues d'une fonction de hachage ? $\Rightarrow$ nombreuses !

- résistance aux collisions
- résistance à la pré-image, seconde pré-image
- résistance aux "near-collisions"
- résistance à la recherche d'entrées $x_1, \ldots, x_k$ telles que $H(x_1) \oplus \cdots \oplus H(x_k) = 0$
- ...

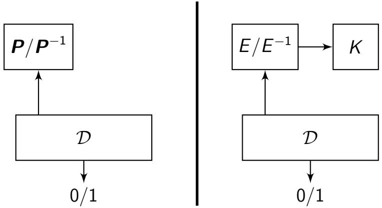
En fait, on attend d'une fonction de hachage qu'elle se "comporte comme" une fonction aléatoire

Le modèle de l'oracle aléatoire (ROM)

- modélise une fonction de hachage comme un oracle publiquement accessible $\boldsymbol{H} : \{0,1\}^* \rightarrow \{0,1\}^n$ retournant une chaine de n bits uniformément aléatoires à chaque nouvelle requête
- introduit par Bellare et Rogaway ('93)
- très utilisé dans les preuves de sécurité, not. clé publique (OAEP, FDH, PSS...)
- résultats d'ininstantiabilité [CanettiGH98, Nielsen02] : il existe des cryptosystèmes prouvés sûrs dans le ROM mais vulnérables avec n'importe quelle fonction de hachage
- schémas prouvés sûrs dans le modèle standard : souvent moins efficaces ou utilisant des hypothèses de complexité moins classiques
    - chiffrement de Cramer-Shoup
    - signatures de Boneh-Boyen...

Chiffrement par blocs, modèle standard

- notion de sécurité standard pour un chiffrement par blocs : permutation pseudo-aléatoire (PRP) ou fortement pseudo-aléatoire (SPRP) = indistinguable d'une permutation aléatoire (inversible pour SPRP)



- la notion de (S)PRP ne prend pas en compte certains modèles d'attaques plus forts : attaques à clés reliées, attaques à clé connues...
- pour prouver la sécurité de certains cryptosystèmes, la seule hypothèse de (S)PRP ne suffit parfois pas (*e.g.* fonctions de hachage fondées sur un chiffrement par blocs)

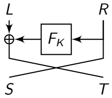
Le modèle du chiffrement idéal (ICM)

- modélise un chiffrement par blocs parfaitement aléatoire comme une paire d'oracles publiquement accessibles $\boldsymbol{E}(\cdot,\cdot)$ et $\boldsymbol{E}^{-1}(\cdot,\cdot)$, tels que $\boldsymbol{E}(K,\cdot)$ est une permutation aléatoire pour chaque clé K
- introduit par [Shannon49, Winternitz84]
- modèle de la permutation aléatoire (RPM) : un seule permutation $\boldsymbol{P}$ et son inverse $\boldsymbol{P}^{-1}$ (= un chiffrement idéal avec une clé fixée)
- moins populaire que le ROM :
    - très utilisé pour analyser les fonctions de hachage fondées sur un chiffrement par blocs, *e.g.* mode Davies-Meyer [BlackRS02, Hirose06]
    - utilisé dans les preuves de sécurités de quelques schémas à clé publique (chiffrement, échange de clé authentifié...)
- résultats d'ininstantiabilité comme pour le ROM [Black06]

Liens ROM - ICM

On peut construire un chiffrement par blocs à partir d'une fonction de hachage et réciproquement :

- étant donné un chiffrement par blocs, on peut construire une fonction de compression (Davies-Meyer, Miyaguchi-Preneel, etc.) puis une fonction de hachage (Merkle-Damgård)
- étant donné une fonction de hachage, on peut construire un chiffrement par blocs avec le schéma de Feistel :



Quelles sont les propriétés de la construction lorsque la primitive sous-jacente est un oracle aléatoire ou un chiffrement par blocs idéal ?

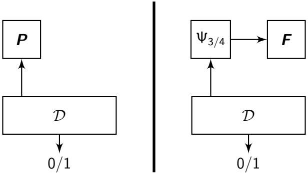
Plan

Indistinguabilité du schéma de Feistel

Théorème

Le schéma de Feistel à trois (resp. quatre) tours avec des fonctions de tour aléatoires est indistinguable d'une permutation aléatoire (resp. permutation aléatoire inversible)

NB : Reste vrai avec des fonctions de tour pseudo-aléatoires.



$\Rightarrow$ tout cryptosystème prouvé sûr avec une permutation aléatoire reste sûr avec un Feistel dont les fonctions de tour sont aléatoires et secrètes.

Limites de l'indistinguabilité

- Comment généraliser le théorème de Luby-Rackoff quand les fonctions de tours sont publiques ?
- Exemple : schéma de chiffrement RSA de Phan-Pointcheval :

$$\mathrm{Enc}_{\mathrm{pk}=(N,e)}(m;r) = (\boldsymbol{P}(m\|r))^e \mod N \quad , \qquad r \text{ aléa}$$

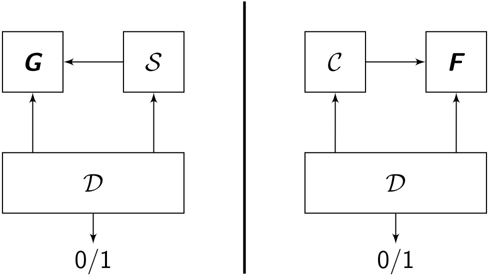
  $\Rightarrow$ prouvé sûr lorsque $\boldsymbol{P}$ est une permutation aléatoire (publique)
- Peut-on remplacer $\boldsymbol{P}$ par un schéma de Feistel à 4 tours avec des fonctions de tour aléatoires et publiques ?
- Luby-Rackoff ne permet pas conclure car l'hypothèse "clé secrète" n'est pas vérifiée

Indifférentiabilité

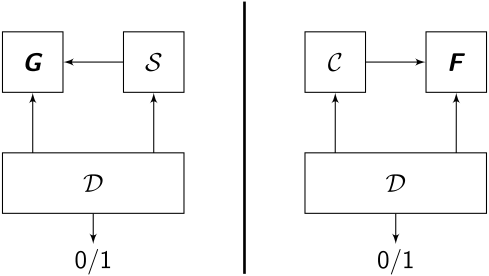
Généralisation de l'indistinguabilité au cas où le distingueur a accès aux composants internes de la construction (= fonctions de tour pour un Feistel).

Définition

$\mathcal{C}^{\boldsymbol{F}}$ est indifférentiable de $\boldsymbol{G}$ s'il existe un simulateur (polynomial) $\mathcal{S}$ tel que les deux systèmes $(\boldsymbol{G}, \mathcal{S}^{\boldsymbol{G}})$ et $(\mathcal{C}^{\boldsymbol{F}}, \boldsymbol{F})$ sont indistinguables.



Indifférentiabilité

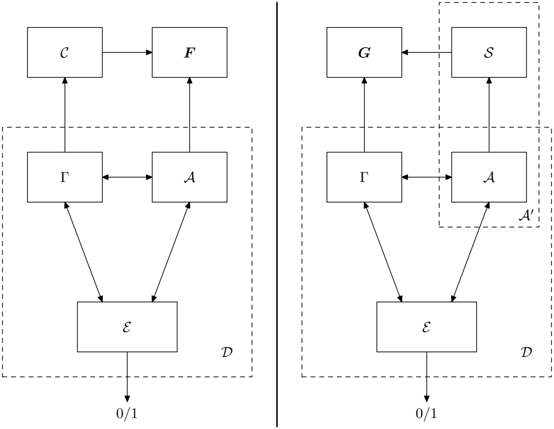


Les réponses du simulateur doivent être :

- cohérentes avec les réponses que $\mathcal{D}$ peut obtenir directement de $\boldsymbol{G}$
- indistinguables de réponses uniformément aléatoires

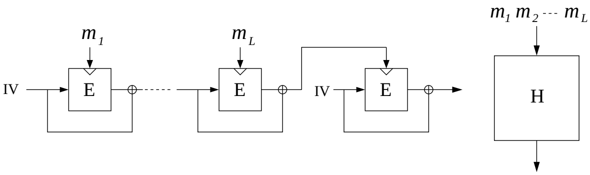
NB : le simulateur n'a pas connaissance des requêtes de $\mathcal{D}$ à $\boldsymbol{G}$.

Théorème de composition



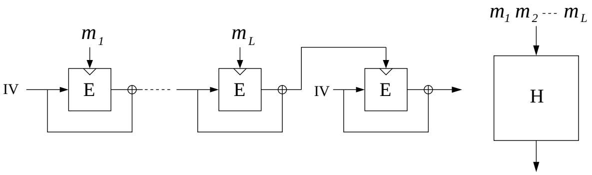
Si $\mathcal{C}^{\boldsymbol{F}}$ est indifférentiable de $\boldsymbol{G}$, alors tout cryptosystème Γ sûr avec $\boldsymbol{G}$ est sûr lorsque $\mathcal{C}^{\boldsymbol{F}}$ remplace $\boldsymbol{G}$.

L'ICM "implique" le ROM



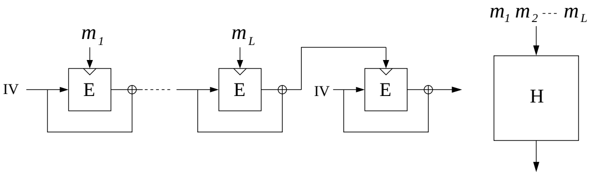
- dans [CoronDMP05], il a été montré que des variantes de Merkle-Damgård utilisée avec un chiffrement idéal en mode Davies-Meyer sont indifférentiables d'un oracle aléatoire
- $\Rightarrow$ une telle construction peut remplacer un oracle aléatoire dans n'importe quel cryptosystème sans perte de sécurité (th. de composition)

L'ICM "implique" le ROM



- dans [CoronDMP05], il a été montré que des variantes de Merkle-Damgård utilisée avec un chiffrement idéal en mode Davies-Meyer sont indifférentiables d'un oracle aléatoire
- $\Rightarrow$ une telle construction peut remplacer un oracle aléatoire dans n'importe quel cryptosystème sans perte de sécurité (th. de composition)
- réciproquement, existe-t-il une construction utilisant un oracle aléatoire indifférentiable d'un chiffrement idéal ?

L'ICM "implique" le ROM

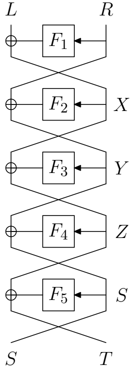


- dans [CoronDMP05], il a été montré que des variantes de Merkle-Damgård utilisée avec un chiffrement idéal en mode Davies-Meyer sont indifférentiables d'un oracle aléatoire
- $\Rightarrow$ une telle construction peut remplacer un oracle aléatoire dans n'importe quel cryptosystème sans perte de sécurité (th. de composition)
- réciproquement, existe-t-il une construction utilisant un oracle aléatoire indifférentiable d'un chiffrement idéal ? $\Rightarrow$ Feistel

Plan

5 tours ne suffisent pas

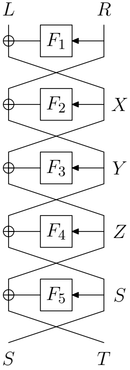
Pour Ψ_5, on peut trouver 4 paires entrées/sorties telles que $R_0 \oplus R_1 \oplus R_2 \oplus R_3 = 0$ et $S_0 \oplus S_1 \oplus S_2 \oplus S_3 = 0$



5 tours ne suffisent pas

Pour Ψ_5, on peut trouver 4 paires entrées/sorties telles que $R_0 \oplus R_1 \oplus R_2 \oplus R_3 = 0$ et $S_0 \oplus S_1 \oplus S_2 \oplus S_3 = 0$

X_{12}

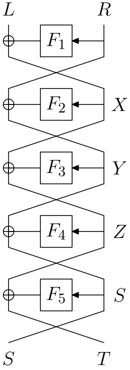


5 tours ne suffisent pas

Pour Ψ_5, on peut trouver 4 paires entrées/sorties telles que
$R_0 \oplus R_1 \oplus R_2 \oplus R_3 = 0$ et $S_0 \oplus S_1 \oplus S_2 \oplus S_3 = 0$

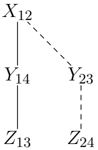
X_{12}

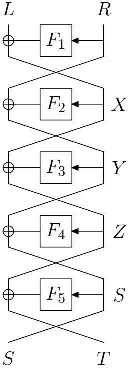
Y_{14} Y_{23}



5 tours ne suffisent pas

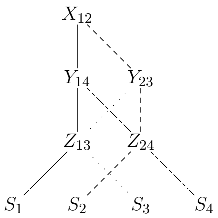
Pour Ψ_5, on peut trouver 4 paires entrées/sorties telles que $R_0 \oplus R_1 \oplus R_2 \oplus R_3 = 0$ et $S_0 \oplus S_1 \oplus S_2 \oplus S_3 = 0$

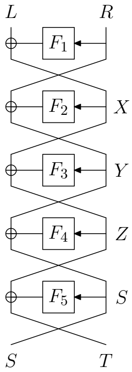




5 tours ne suffisent pas

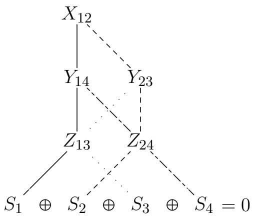
Pour Ψ_5, on peut trouver 4 paires entrées/sorties telles que
$R_0 \oplus R_1 \oplus R_2 \oplus R_3 = 0$ et $S_0 \oplus S_1 \oplus S_2 \oplus S_3 = 0$

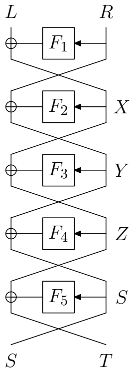




5 tours ne suffisent pas

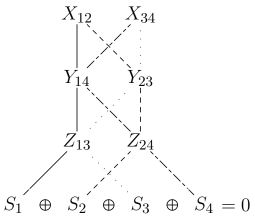
Pour Ψ_5, on peut trouver 4 paires entrées/sorties telles que $R_0 \oplus R_1 \oplus R_2 \oplus R_3 = 0$ et $S_0 \oplus S_1 \oplus S_2 \oplus S_3 = 0$

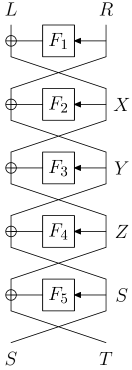




5 tours ne suffisent pas

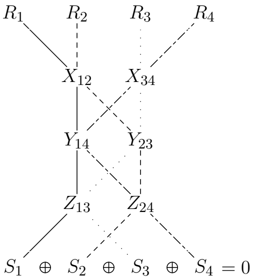
Pour Ψ_5, on peut trouver 4 paires entrées/sorties telles que $R_0 \oplus R_1 \oplus R_2 \oplus R_3 = 0$ et $S_0 \oplus S_1 \oplus S_2 \oplus S_3 = 0$

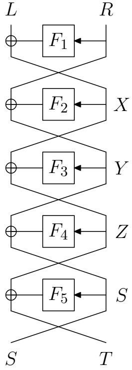




5 tours ne suffisent pas

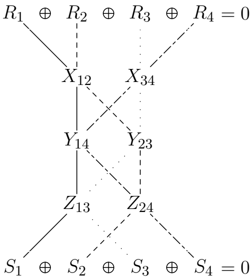
Pour Ψ_5, on peut trouver 4 paires entrées/sorties telles que $R_0 \oplus R_1 \oplus R_2 \oplus R_3 = 0$ et $S_0 \oplus S_1 \oplus S_2 \oplus S_3 = 0$

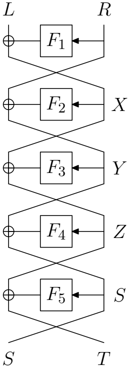




5 tours ne suffisent pas

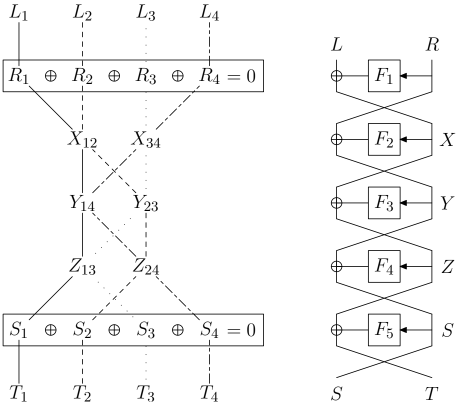
Pour Ψ_5, on peut trouver 4 paires entrées/sorties telles que $R_0 \oplus R_1 \oplus R_2 \oplus R_3 = 0$ et $S_0 \oplus S_1 \oplus S_2 \oplus S_3 = 0$





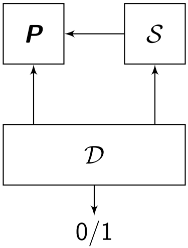
5 tours ne suffisent pas

Pour Ψ_5, on peut trouver 4 paires entrées/sorties telles que $R_0 \oplus R_1 \oplus R_2 \oplus R_3 = 0$ et $S_0 \oplus S_1 \oplus S_2 \oplus S_3 = 0$



5 tours ne suffisent pas

- pour une permutation aléatoire, trouver 4 paires entrées/sorties telles que $R_0 \oplus R_1 \oplus R_2 \oplus R_3 = 0$ et $S_0 \oplus S_1 \oplus S_2 \oplus S_3 = 0$ est impossible en temps polynomial
- par conséquent, si $\mathcal{D}$ interagit avec $(\boldsymbol{P}, \mathcal{S}^{\boldsymbol{P}})$, le simulateur $\mathcal{S}$ ne peut pas être cohérent avec la permutation aléatoire



Plan

Indifférentiabilité du schéma de Feistel

Théorème (Holenstein *et al.*, STOC 2011)

La construction de Feistel à 14 tours (avec des fonctions de tour parfaitement aléatoires) est indifférentiable d'une permutation aléatoire inversible.

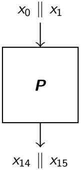
- on obtient un chiffrement par blocs idéal en concaténant la clé à l'entrée de chaque fonction de tour ($F_{i,K}(x) = H(i\|K\|x)$)
- preuve : il faut construire un simulateur

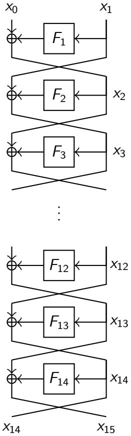
Simulation : stratégie générale

- Rappel : le simulateur doit renvoyer des réponses :
    - cohérentes avec $\boldsymbol{P}$:

$$\forall x_0, x_1, \ \Psi_{14}(x_0, x_1) = \boldsymbol{P}(x_0, x_1)$$

    - indistinguables de réponses unif. aléatoires
- le simulateur maintient un historique de valeurs pour chaque F_i
- lorsque le distingueur fait une requête $F_i(x_i)$, le simulateur complète certaines "chaines" par avance





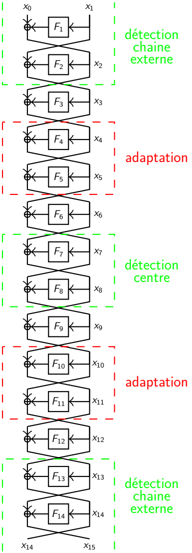
Simulation : stratégie générale

- Le simulateur complète deux types de chaines :
  - les centres (x_7, x_8)
  - les chaines externes (x_1, x_2) ou (x_{13}, x_{14}) telles que :

$$\boldsymbol{P}(x_0, x_1) = (x_{14}, x_{15}),$$

  où $x_0 = x_2 \oplus F_1(x_1)$ et $x_{15} = x_{13} \oplus F_{14}(x_{14})$

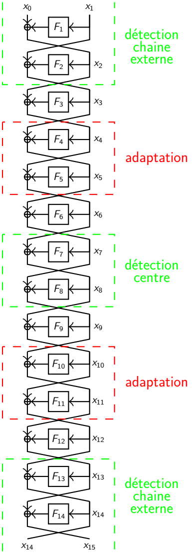
- Ces chaines sont "adaptées" en F_4, F_5 ou F_{10}, F_{11} pour "coller" avec la permutation aléatoire $\boldsymbol{P}$



Adaptation

- Lorsque le simulateur détecte un centre (x_7, x_8) lors de la requête $F_7(x_7)$:
  - il prolonge la chaine en avant en définissant les fonctions de tour aléatoirement et en faisant un appel à $\boldsymbol{P}$:

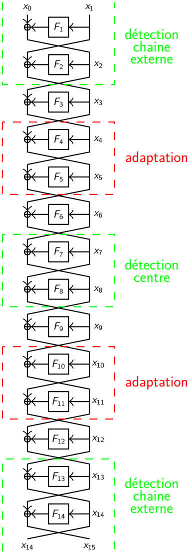
$$
\begin{aligned}
x_9 &= x_7 \oplus F_8(x_8) \\
x_{10} &= x_8 \oplus F_9(x_9) \\
&\vdots \\
(x_0, x_1) &= \boldsymbol{P}^{-1}(x_{14}, x_{15}) \\
&\vdots \\
x_4 &= x_2 \oplus F_3(x_3)
\end{aligned}
$$



Adaptation

- Lorsque le simulateur détecte un centre (x_7, x_8) lors de l'ajout de x_7 :
  - il prolonge la chaine en arrière en définissant les fonctions de tour aléatoirement :

$$x_6 = x_8 \oplus F_7(x_7)$$
$$x_5 = x_7 \oplus F_6(x_6)$$



Adaptation

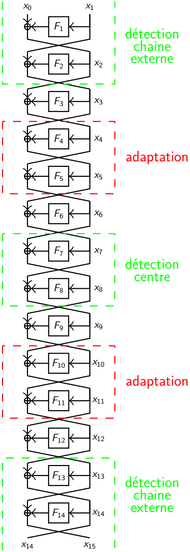
- Lorsque le simulateur détecte un centre (x_7, x_8) lors de l'ajout de x_7 :
  - il prolonge la chaine en arrière en définissant les fonctions de tour aléatoirement :

$$x_6 = x_8 \oplus F_7(x_7)$$
$$x_5 = x_7 \oplus F_6(x_6)$$

  - il adapte la chaine en définissant :

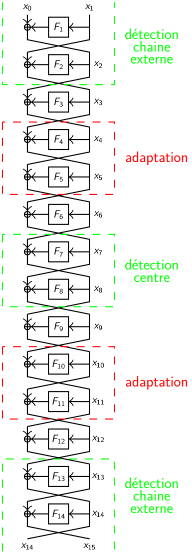
$$F_4(x_4) = x_3 \oplus x_5$$
$$F_5(x_5) = x_4 \oplus x_6$$

  de façon à ce que $\Psi_{14}(x_0, x_1) = \boldsymbol{P}(x_0, x_1)$



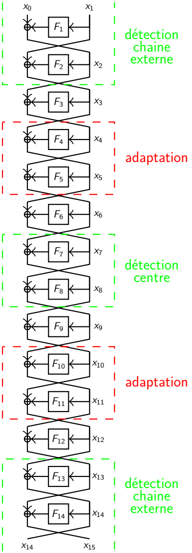
Adaptation

- symétrique si détection lors de l'ajout de x_8
- similaire pour compléter une chaine externe (x_1, x_2) ou (x_{13}, x_{14})



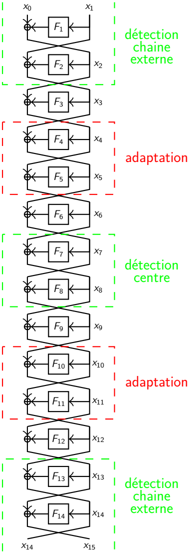
Ce qui pourrait faire échouer le simulateur. . .

- *temps d'exécution exponentiel dû à la complétion récursive des chaines* :
  - compléter un centre peut créer de nouvelles chaines externes. . .
  - compléter une chaine externe crée de nouveaux centres. . .
  - etc.



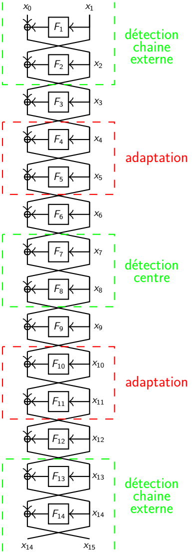
Ce qui pourrait faire échouer le simulateur...

- *temps d'exécution exponentiel dû à la complétion récursive des chaines* :
  - compléter un centre peut créer de nouvelles chaines externes...
  - compléter une chaine externe crée de nouveaux centres...
  - etc.
- *impossibilité de s'adapter* :
  - si la valeur en laquelle le simulateur doit s'adapter est déjà dans l'historique de F_i, impossibilité de rester cohérent avec $\boldsymbol{P}$



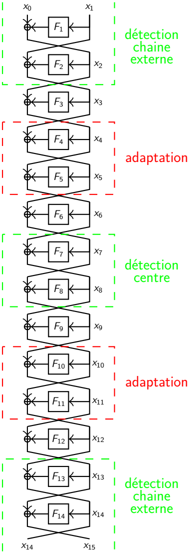
Exécution en temps polynomial

- Rappel : le distingueur fait au plus un nombre polynomial q de requêtes



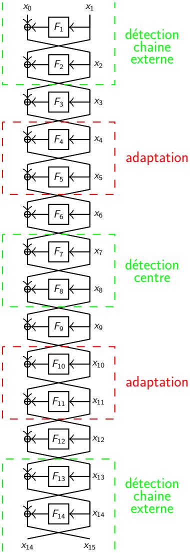
Exécution en temps polynomial

- Rappel : le distingueur fait au plus un nombre polynomial q de requêtes
- Remarque cruciale : une chaine externe ne peut être crée que si le distingueur a fait la requête correspondante à $\boldsymbol{P}$
  $\Rightarrow$ nombre inférieur à q



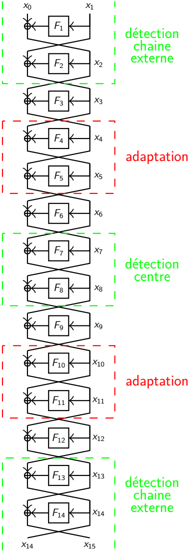
Exécution en temps polynomial

- Rappel : le distingueur fait au plus un nombre polynomial q de requêtes
- Remarque cruciale : une chaine externe ne peut être crée que si le distingueur a fait la requête correspondante à $\boldsymbol{P}$
  $\Rightarrow$ nombre inférieur à q
- implique que la taille des historiques de F_7 et F_8 est inférieure à $2q$



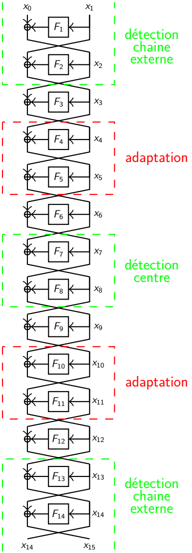
Exécution en temps polynomial

- Rappel : le distingueur fait au plus un nombre polynomial q de requêtes
- Remarque cruciale : une chaine externe ne peut être crée que si le distingueur a fait la requête correspondante à $\boldsymbol{P}$
  $\Rightarrow$ nombre inférieur à q
- implique que la taille des historiques de F_7 et F_8 est inférieure à $2q$
- et par conséquent le nombre de centres complétés est $\leq 4q^2$



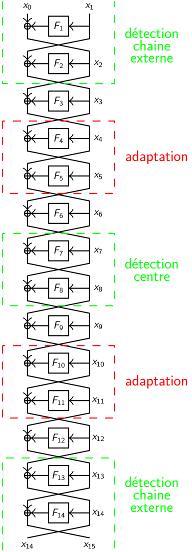
Le simulateur peut toujours s'adapter

- ex : détection d'un centre (x_7, x_8) lors de l'ajout de x_7
  $\Rightarrow$ adaptation en F_4 et F_5



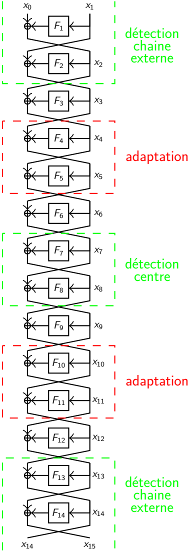
Le simulateur peut toujours s'adapter

- ex : détection d'un centre (x_7, x_8) lors de l'ajout de x_7
  $\Rightarrow$ adaptation en F_4 et F_5
- prolongation chaine arrière :
  $x_5 = x_7 \oplus F_6(x_6)$ est uniformément distribué, donc dans l'historique de F_5 avec proba. négligeable



Le simulateur peut toujours s'adapter

- ex : détection d'un centre (x_7, x_8) lors de l'ajout de x_7
  $\Rightarrow$ adaptation en F_4 et F_5
- prolongation chaine arrière :
  $x_5 = x_7 \oplus F_6(x_6)$ est uniformément distribué, donc dans l'historique de F_5 avec proba. négligeable
- prolongation chaine avant : x_3 ne peut pas être dans l'historique de F_3 sinon la chaine externe (x_1, x_2) aurait déjà été détectée et complétée
  $\Rightarrow x_4 = x_2 \oplus F_3(x_3)$ est uniformément distribué, donc dans l'historique de F_4 avec proba. négligeable



Applications

- Résultat principalement théorique sur la possibilité de construire un oracle de permutation à partir d'un oracle de fonction.

Applications

- Résultat principalement théorique sur la possibilité de construire un oracle de permutation à partir d'un oracle de fonction.
- Dans la pratique, une analyse dédiée est souvent plus efficace que remplacer génériquement une permutation aléatoire par un Feistel à 14 tours.

Applications

- Résultat principalement théorique sur la possibilité de construire un oracle de permutation à partir d'un oracle de fonction.
- Dans la pratique, une analyse dédiée est souvent plus efficace que remplacer génériquement une permutation aléatoire par un Feistel à 14 tours.
- exemple du schéma de chiffrement RSA de Phan-Pointcheval :

$$\mathrm{Enc}_{\mathrm{pk}=(N,e)}(m;r) = (\boldsymbol{P}(m\|r))^e \mod N \quad , \quad r \text{ aléa}$$

$\Rightarrow$ ***P*** peut en fait être remplacée par un Feistel à 3 tours et le schéma reste prouvé sûr dans le ROM

Applications

- Résultat principalement théorique sur la possibilité de construire un oracle de permutation à partir d'un oracle de fonction.
- Dans la pratique, une analyse dédiée est souvent plus efficace que remplacer génériquement une permutation aléatoire par un Feistel à 14 tours.
- exemple du schéma de chiffrement RSA de Phan-Pointcheval :

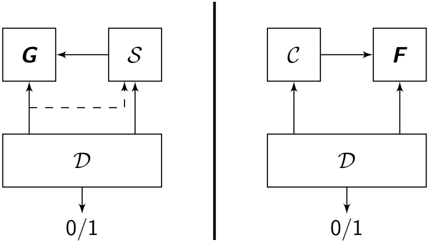
$$\mathrm{Enc}_{\mathrm{pk}=(N,e)}(m;r) = (\boldsymbol{P}(m\|r))^e \mod N \quad , \quad r \text{ aléa}$$

  $\Rightarrow$ $\boldsymbol{P}$ peut en fait être remplacée par un Feistel à 3 tours et le schéma reste prouvé sûr dans le ROM
- exemple du chiffrement de Even-Mansour : $E_{k_1,k_2}(m) = k_2 \oplus \boldsymbol{P}(m \oplus k_1)$
  - sûr lorsque $\boldsymbol{P}$ est une permutation aléatoire
  - reste sûr dans le ROM avec un Feistel à 4 tours [GentryR04]

Plan

Indifférentiabilité publique

Affaiblissement du modèle de l'indifférentiabilité générale : le simulateur a connaissance des requêtes de $\mathcal{D}$ à $\boldsymbol{G}$



Le théorème de composition est valable pour les cryptosystèmes où toutes les requêtes à la primitive $\boldsymbol{G}$ sont publiques (*e.g.* requêtes de hachage dans la majorité des schémas de signature).

Indifférentiabilité publique du schéma de Feistel

Théorème (MandalPS12)

Le schéma de Feistel à 6 tours (avec des fonctions de tour aléatoires) est publiquement indifférentiable d'une permutation aléatoire inversible (et 6 et le nombre de tours minimal pour avoir cette propriété).

Preuve beaucoup plus simple que pour l'indifférentiabilité générale.

Résistance à la corrélation

Une construction $\mathcal{C}^{\boldsymbol{F}}$ est résistante à la corrélation (par rapport à la primitive idéale $\boldsymbol{G}$) si toute relation entré-sortie difficile à trouver pour $\boldsymbol{G}$ (appelée relation évasive) est difficile à trouver pour $\mathcal{C}^{\boldsymbol{F}}$ (même en ayant accès à $\boldsymbol{F}$).

Exemple : pour une permutation aléatoire inversible $\boldsymbol{P}$ sur $2n$ bits, la relation suivante est évasive :

$$\{(L\|R, S\|T) \,:\, L = 0^n \text{ et } S = 0^n\}$$

NB : Notion impossible à satisfaire dans le modèle standard.

Théorème

Si $\mathcal{C}^{\boldsymbol{F}}$ est publiquement indifférentiable de $\boldsymbol{G}$, alors $\mathcal{C}^{\boldsymbol{F}}$ est résistante à la corrélation.

Conclusion

Notion	nbre de tours de Feistel
PRP	3
SPRP	4
Résistance à la corrél.	6
Indiff. publique	6
Indiff. générale	entre 6 et 14

- les résultats d'indifférentiabilité ne sont valables qu'avec des fonctions de tour aléatoires
  $\Rightarrow$ pas applicable à DES (fonctions de tour trop simples)

Conclusion

Notion	nbre de tours de Feistel
PRP	3
SPRP	4
Résistance à la corrél.	6
Indiff. publique	6
Indiff. générale	entre 6 et 14

- les résultats d'indifférentiabilité ne sont valables qu'avec des fonctions de tour aléatoires
  $\Rightarrow$ pas applicable à DES (fonctions de tour trop simples)
- le résultat ne dit rien sur la possibilité d'instancier un chiffrement idéal avec AES ou un oracle aléatoire avec SHA-2

Conclusion

Notion	nbre de tours de Feistel
PRP	3
SPRP	4
Résistance à la corrél.	6
Indiff. publique	6
Indiff. générale	entre 6 et 14

- les résultats d'indifférentiabilité ne sont valables qu'avec des fonctions de tour aléatoires
  $\Rightarrow$ pas applicable à DES (fonctions de tour trop simples)
- le résultat ne dit rien sur la possibilité d'instancier un chiffrement idéal avec AES ou un oracle aléatoire avec SHA-2
- principal problème ouvert : nombre optimal de tours pour l'indifférentiabilité générale ? (entre 6 et 14)

The end. . .

Merci de votre attention !
Commentaires ou questions ?