Preuves de sécurité en cryptographie symétrique à l'aide de la technique du coupling

Rodolphe Lampe

Université de Versailles Saint-Quentin-en-Yvelines
UFR de Sciences - École doctorale STV - Laboratoire PRiSM

Preuves de sécurité en cryptographie symétrique à l'aide de la technique du coupling

THÈSE

présentée pour l'obtention du grade de

Docteur de l'Université de Versailles Saint-Quentin-en-Yvelines

(Spécialité Informatique)

par

Rodolphe LAMPE

Soutenue publiquement le 2 décembre 2014 devant le jury composé de

Jean-Sébastien Coron (Univ. du Luxembourg)	*Rapporteur*
David Naccache (ENS Paris)	*Rapporteur*
Jacques Patarin (Univ. de Versailles)	*Directeur*
Louis Goubin (Univ. de Versailles)	*Examinateur*
Antoine Joux (Univ. de Paris 6, CryptoExperts)	*Examinateur*
David Pointcheval (ENS Paris)	*Examinateur*
Yannick Seurin (ANSSI)	*Examinateur*

Remerciements

C'est avec un grand plaisir que je tiens à remercier, en premier lieu, mon directeur de thèse, Jacques Patarin qui, avec beaucoup de gentillesse et de bienveillance, a dirigé mon travail durant cette thèse. J'admire sa créativité, sa curiosité, la richesse de ses idées et la persévérance dont il fait preuve pour s'attaquer à des problèmes difficiles comme la théorie des Miroirs qu'il a fondée. J'ai également apprécié la confiance qu'il a placée en moi en me laissant l'autonomie et la liberté dont j'ai tant besoin, ce qui m'a permis de m'épanouir autant professionnellement que personnellement.

J'ai une profonde gratitude pour Yannick Seurin, avec qui j'ai pris beaucoup de plaisir à travailler. Je suis très reconnaissant de toute l'aide et du temps que Yannick m'a consacrés pour m'aider à améliorer ma rédaction, travailler ensemble et me guider vers des sujets qui ont été très porteurs, comme le coupling et le schéma d'Even-Mansour.

C'est une belle et enrichissante expérience qui m'a permis de rencontrer et d'échanger avec de nombreux collègues cryptologues que je remercie : en particulier Joana Treger, Thomas Peyrin, Cécile Goncalves, Jean-Christophe Zapalowicz, Jérémy Jean, Léo Ducas, Christina Boura, Luca De Feo, Nicolas Gama, Michaël Quisquater, Henri Gilbert, Emmanuel Volte, Valérie Nachef, Benoit Cogliati, Cyril Hugounenq, Anja Becker, Maria Plasencia, Olivier Billet, ...

Dans la périlleuse aventure des démarches administratives, un grand merci également à Louis Goubin pour son aide précieuse, ainsi que pour ses conseils avisés. Je souhaite aussi remercier Catherine Le-Quere et Veronique Delahaye qui m'ont aidé pour ces démarches.

Je remercie mes rapporteurs qui ont accepté de relire cette thèse : David Naccache et Jean-Sébastien Coron. Je remercie également Louis Goubin, Antoine Joux, David Pointcheval et Yannick Seurin qui ont bien voulu participer à mon jury de thèse. Je remercie la Direction Générale de l'Armement (DGA) ainsi que l'Agence Nationale de la Recherche (ANR) qui ont financé ma thèse.

Enfin, ce message de remerciement s'achève avec une chaleureuse pensée pour ma famille et mes amis. Je remercie plus particulièrement Clémence qui m'a toujours encouragé et soutenu dans ce travail, qui m'a beaucoup aidé à corriger ma thèse ainsi qu'à concevoir le message « crypté » qui se cache dans ces remerciements... (saurez-vous le trouver ? !) J'ai aussi une pensée particulière pour ma prof de français de troisième qui voulait m'envoyer en BEP, finalement j'ai décidé de pousser un peu plus loin les études ...☺ Pour terminer, je dédie cette thèse à mon petit garçon Charlie qui est arrivé sur cette terre pour ponctuer en beauté cette fin de thèse !

Attention Alice et Bob, Charlie arrive !

Table des matières

Table des figures

Liste des tableaux

Notations

$\mathcal{I}_n$	ensemble des chaînes de bits de longueur n
$(S)^{*q}$	ensemble des $(x_1, \ldots, x_n) \in S^q$ vérifiant $x_i \neq x_j, \forall i \neq j$
$(N)_q$	$N(N-1)\cdots(N-q+1)$
$[i; j]$	ensemble des entiers k tels que $i \leq k \leq j$
$\mathrm{Perm}(\mathcal{D})$	ensemble des permutations d'un ensemble $\mathcal{D}$
$\mathcal{P}_n$	ensemble des permutations de $\mathcal{I}_n$
$\mathcal{F}_n$	ensemble des fonctions de $\mathcal{I}_n$ dans $\mathcal{I}_n$
$\mathsf{BC}(\mathcal{K}, \mathcal{D})$	ensemble des schémas de chiffrement ayant pour domaine $\mathcal{D}$ et pour espace des clés $\mathcal{K}$
E_k	la permutation $E(k, \cdot)$ où $E \in \mathsf{BC}(\mathcal{K}, \mathcal{D})$ et $k \in \mathcal{K}$
E^*	le schéma de chiffrement parfait : $\forall \pi \in \mathcal{P}_n, E^*(\pi, \cdot) = \pi(\cdot)$
$\mathcal{O}$	oracle
$\mathcal{A}$	attaquant
Ω	espace de probabilité
$x \leftarrow_{\$} X$	une valeur est tirée uniformément aléatoire dans l'ensemble X et assignée à x
$\Pr[event]$	probabilité d'un évènement *event*
Adv	avantage d'indistinguabilité
ncpa	attaque à clairs choisis, non-adaptative (non-adaptative chosen plaintext attack)
cca	attaque à clairs et chiffrés choisis, adaptative (chosen-ciphertext attack)
$\|\mu - \nu\|$	distance statistique entre deux distributions de probabilités μ et ν

Introduction

Durant des siècles, la cryptologie a consisté en un aller-retour entre l'invention d'un nouveau procédé de chiffrement (cryptographie) et l'attaque de celui-ci (cryptanalyse), imposant d'en inventer un autre plus performant. L'évolution de la cryptologie peut être comparée à l'évolution de l'architecture : on a d'abord construit des ponts en les améliorant en fonction de leur solidité éprouvée, jusqu'au jour où les connaissances mathématiques et physiques ont été suffisamment évoluées pour prévoir et calculer la solidité d'un pont avant de le construire, permettant ainsi d'anticiper les problèmes et de s'assurer de la solidité du pont. En cryptographie, cette capacité à prouver la sécurité d'un schéma débute avec la théorie de l'information de Shanon dans son article *Communication theory of secrecy systems* paru en 1949.

Dans les années qui ont suivi, la sécurité prouvée a continué de se développer vers plus de formalisme mathématique et, aujourd'hui, les preuves de sécurité reposent énormément sur des calculs probabilistes et une rigueur très mathématique. Les cryptologues cherchent à prouver que certains schémas se comportent quasiment comme des objets idéalisés (par exemple une permutation aléatoire ou une famille de permutations aléatoires) qui ont une sécurité parfaite car les messages chiffrés ne révèlent aucune information sur les messages clairs. Pour étudier de quelle façon un schéma est plus ou moins proche d'un objet idéalisé, on introduit la notion d'« indistinguabilité », qui permet de mesurer la difficulté à distinguer un schéma d'un objet idéal. Avec cette notion, il est alors possible de transposer l'étude de la sécurité d'un schéma à un ensemble de calculs de probabilités, généralement compliqués.

Dans cette thèse, on s'intéresse à des schémas de chiffrement par blocs, c'est-à-dire que le chiffrement (et le déchiffrement) envoie un bloc de n bits sur un bloc de n bits et, puisque le déchiffrement est la fonction inverse du chiffrement, les fonctions de chiffrements sont vues comme des familles de permutations sur $\{0,1\}^n$. Il y a essentiellement deux grandes structures utilisées pour un schéma de chiffrement par blocs : la structure de Feistel (utilisée pour le DES) et la structure SPN (utilisée pour l'AES). L'étude de la sécurité de ces différentes structures et schémas a permis de nombreuses avancées autant pratiques que théoriques. Ainsi, Luby et Rackoff [LR86] ont prouvé l'indistinguabilité du schéma de Feistel à 3 tours (pour un attaquant limité à des requêtes directes), Jacques Patarin a inventé la technique des coefficients H qui permet, entre autres, d'améliorer et de prouver de nombreuses bornes de sécurité pour les schémas de Feistel à 4, 5 et 6 tours [Pat90, Pat91, Pat98, Pat03, Pat04], Kilian et Rogaway [KR96] ont largement utilisé et formalisé la technique de preuve par jeux, Serge Vaudenay a inventé la théorie de la décorrélation pour prouver la sécurité d'un schéma face à des attaques différentielles ou linéaires [Vau98], Ueli Maurer a inventé la théorie des Random Systems et a prouvé la sécurité des schémas de Feistel avec un nombre arbitraire de tours [Mau02, MP03], etc.

En 2002, Mironov [Mir02] a utilisé une technique du domaine des probabilités, le coupling et le temps de mixage des chaînes de Markov, pour étudier la distribution de probabilité des sorties de l'algorithme de génération de clé du schéma de chiffrement RC4. Cette puissante technique a ensuite été utilisée pour obtenir d'autres preuves de sécurité, par Morris *et al.* [MRS09] pour l'analyse des schémas de Feistel maximalement non-balancés,

et par Hoang et Rogaway [HR10] pour l'analyse des schémas de Feistel balancés, non-balancés et généralisés. Dans cette thèse, nous nous sommes inspirés du travail de Morris *et al.* [MRS09] et Hoang et Rogaway [HR10] pour appliquer la technique du coupling à de nouveaux schémas : Even-Mansour itéré (Lampe, Patarin et Seurin [LPS12]), CLRW (Lampe et Seurin [LS13b]), Feistel à clés alternées (Lampe et Seurin [LS14]). Dans un premier chapitre, nous présentons quelques généralités et définitions sur les preuves de sécurité en cryptographie. Puis, nous présentons la technique du coupling appliquée aux preuves de sécurité (chapitre 2) et son utilisation pour le schéma d'Even-Mansour itéré (chapitre 3), le schéma CLRW (chapitre 4) et le schéma de Feistel à clés alternées (chapitre 5). Nous poursuivons sur l'étude du schéma d'Even-Mansour à deux tours pour certaines minimisations (pour des clés de tours identiques ou des permutations internes identiques par exemple) au chapitre 6 (qui correspond aux résultats de Chen, Lampe, Lee, Seurin et Steinberber [CLL$^+$14]). Enfin, nous concluons sur une comparaison des différentes techniques d'indistinguabilité au chapitre 7.

Au cours de cette thèse, nous avons également proposé et étudié une extension du schéma PKP d'Adi Shamir (Lampe et Patarin [LP12]), prouvé l'indifférentiabilité du schéma d'Even-Mansour à 12 tours (Lampe et Seurin [LS13a]) et amélioré les bornes de sécurité pour l'indistinguabilité du xor de k bijections (Cogliati, Lampe et Patarin [CLP14]) mais ces articles ne sont pas présentés dans ce manuscrit.

Articles publiés durant cette thèse

(En gras, les articles exposés dans ce manuscrit)

[CLL+14] **Shan Chen, Rodolphe Lampe, Jooyoung Lee, Yannick Seurin and John P. Steinberger.**
Minimizing the Two-Round Even-Mansour Cipher.
In *Advances in Cryptology - CRYPTO 2014*.

[LS14] **Rodolphe Lampe and Yannick Seurin.**
Security Analysis of Key-Alternating Feistel Ciphers.
In *Fast Software Encryption - FSE 2014*.

[CLP14] Benoit Cogliati, Rodolphe Lampe and Jacques Patarin.
The Indistinguishability of the xor of k permutations.
In *Fast Software Encryption - FSE 2014*.

[LS13*b*] Rodolphe Lampe and Yannick Seurin.
How to Construct an Ideal Cipher from a Small Set of Public Permutations.
In *Advances in Cryptology - ASIACRYPT 2013*.

[LS13*a*] **Rodolphe Lampe and Yannick Seurin.**
Tweakable Blockciphers with Asymptotically Optimal Security.
In *Fast Software Encryption - FSE 2013*.

[LPS12] **Rodolphe Lampe, Jacques Patarin, and Yannick Seurin.**
An Asymptotically Tight Security Analysis of the Iterated Even-Mansour Cipher.
In *Advances in Cryptology - ASIACRYPT 2012*.

[LP12] Rodolphe Lampe and Jacques Patarin.
Analysis of some natural variants of the pkp algorithm.
In *SECRYPT 2012*.

Chapitre 1

Preuves de sécurité en cryptographie

1.1 Utilisation d'un schéma de chiffrement pour communiquer

Pendant des siècles, la cryptographie a eu pour principal objectif de permettre des communications « sûres ». Ainsi, Jules César utilisait un chiffrement par décalage : pour envoyer un message M à un allié, il décalait toutes les lettres d'un certain nombre de crans, défini auparavant avec l'allié, et envoyait le message ainsi crypté. Par exemple, pour un décalage de deux crans : A devient C, B devient D, ..., Y devient A et Z devient B. L'allié n'avait alors qu'à déchiffrer le message en décalant dans l'autre sens les lettres (C devient A, D devient B, etc). Bien sûr, ce chiffrement rudimentaire n'est pas sûr car les messages chiffrés révèlent de l'information sur le message clair : on connaît par exemple la taille du message et la présence de lettres qui se répètent. En utilisant la fréquence des lettres, il est possible de déchiffrer le message assez facilement. Dans cet exemple, on voit que Jules César a choisi un secret (le nombre de lettres à décaler), l'a transmis à son allié, a ensuite utilisé un procédé de chiffrement (le décalage) pour rendre son message illisible, puis l'allié a utilisé un processus de déchiffrement (le décalage dans l'autre sens) pour retrouver le message. Cette façon de faire est représentée dans la figure 1.1. Elle représente la manière dont Alice et Bob utilisent la cryptographie dite « symétrique » (car Alice et Bob utilisent la même clé) pour communiquer.

Que demande-t-on à un processus de chiffrement pour que la communication soit « sûre » ? Intuitivement, on veut que le message chiffré ne révèle pas d'information sur le message clair, c'est ce qu'on appelle la « sécurité sémantique ». Avant de formaliser différentes notions de sécurité, nous introduisons la notion de schéma de chiffrement par blocs.

1.2 Schémas de chiffrement par blocs

Pour deux ensembles $\mathcal{D}$ et $\mathcal{K}$, on note $\mathrm{Perm}(\mathcal{D})$ l'ensemble des permutations de $\mathcal{D}$ et $\mathsf{BC}(\mathcal{K}, \mathcal{D})$ l'ensemble des schémas de chiffrement ayant pour domaine $\mathcal{D}$ et pour espace

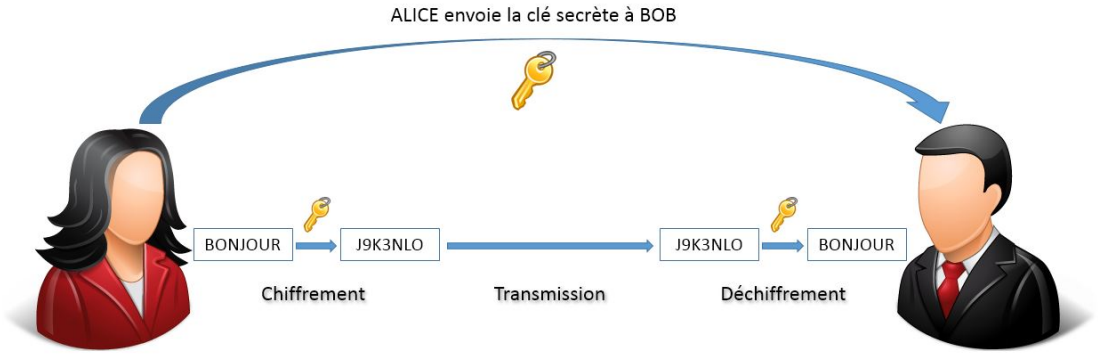

FIGURE 1.1 – Cryptographie symétrique

des clés $\mathcal{K}$, c'est-à-dire l'ensemble des fonctions $E : \mathcal{K} \times \mathcal{D} \to \mathcal{D}$ telles que, pour tout $k \in \mathcal{K}$, $E_k := E(k, \cdot) \in \mathrm{Perm}(\mathcal{D})$. Dans cette thèse, on considère uniquement des schémas de chiffrement symétriques, c'est-à-dire que la clé k permet à la fois de chiffrer et de déchiffrer et elle est partagée entre deux (ou plus) personnes pour pouvoir communiquer de manière plus ou moins sécurisée suivant la solidité du schéma utilisé. Les schémas de chiffrements que nous étudions sont dits « par blocs » car le domaine $\mathcal{D}$ est, typiquement, l'ensemble des chaînes de n bits (pour $n = 128$ par exemple, comme pour le célèbre schéma AES), c'est-à-dire l'ensemble des blocs de n bits.

1.3 Indistinguabilité et distance statistique

1.3.1 Notations et schéma de chiffrement parfait

Le *schéma de chiffrement parfait* sur $\mathcal{D}$ est défini comme le schéma de chiffrement E^* ayant pour espace des clés $\mathrm{Perm}(\mathcal{D})$ et vérifiant, pour tout $\pi \in \mathrm{Perm}(\mathcal{D})$: $E^*_\pi = \pi$. Ce schéma offre une sécurité parfaite puisque chaque message chiffré est uniformément aléatoire et ne révèle aucune information sur le message clair. En effet, pour chaque message clair, le message chiffré a la même distribution : la distribution uniforme. Si ce schéma est parfait, pourquoi ne pas l'utiliser ?

La perfection a un prix et ce prix, c'est la taille de l'espace des clés qui est de $|\mathcal{D}|!$ ce qui rend ce schéma inutilisable pour les domaines utilisés habituellement. L'un des objectifs de la cryptographie est de construire un schéma de chiffrement ayant un espace des clés de taille raisonnable (par exemple, le schéma de chiffrement le plus connu, AES, utilise des clés de 128, 192 ou 256 bits) tout en se comportant le plus possible comme le schéma de chiffrement parfait. Mais que signifie « se comporter le plus possible comme » ?

1.3.2 Définition de l'indistinguabilité

Pour étudier et mesurer plus précisément ce comportement plus ou moins proche de l'idéal, on utilise la notion d'indistinguabilité. Avant de rentrer dans plus de formalisme, nous présentons l'exemple du test de Turing : imaginez que l'on vous propose de discuter, par claviers interposés, avec soit un être humain soit une intelligence artificielle. On ne vous dit pas à qui vous avez affaire et vous devez deviner avec qui vous discutez. Si la

probabilité que vous trouviez la bonne réponse est 1/2, c'est-à-dire aussi « bien » qu'en devinant au hasard, on peut dire que cette intelligence artificielle se comporte aussi bien qu'un être humain. Si la probabilité que vous trouviez la bonne réponse est proche de 1, on peut dire que cette intelligence artificielle ne se comporte pas comme un être humain. Cette approche permet d'étudier un problème qualitatif (comportement plus ou moins proche d'un autre) de manière quantitative (probabilités plus ou moins proches).

En formalisant, vous interagissez avec un oracle $\mathcal{O}$ (c'est-à-dire une « boîte noire » qui peut envoyer et recevoir des informations mais ne révèle rien de son fonctionnement interne) qui répond à vos questions et se comporte soit comme un être humain H soit comme une intelligence artificielle IA. Après avoir interagi avec cet oracle $\mathcal{O}$, vous émettez un bit $b = 0$ ou 1 qui correspond à votre avis (par exemple $b = 1$ si vous pensez que c'est un être humain et 0 sinon). Notons $\Pr[b = 1 : \mathcal{O} = H]$ la probabilité que vous répondiez 1 si l'oracle est un être humain et $\Pr[b = 1 : \mathcal{O} = IA]$ la probabilité que vous répondiez 1 si l'oracle est une intelligence artificielle. On définit votre avantage pour distinguer H de IA par la valeur $|\Pr[b = 1 : \mathcal{O} = H] - \Pr[b = 1 : \mathcal{O} = IA]|$. Plus l'intelligence artificielle est performante et se comporte comme un être humain, et plus votre avantage sera faible. Et inversement.

Revenons maintenant aux schémas de chiffrement. Soit E un schéma de chiffrement et $\mathcal{O}$ un oracle se comportant soit comme E soit comme E^* (le schéma de chiffrement parfait). Soit $\mathcal{A}$ un attaquant souhaitant découvrir si $\mathcal{O}$ se comporte comme E ou comme E^*. Nous considérons toujours que l'attaquant est non borné calculatoirement. On autorise l'attaquant à effectuer un nombre entier q de requêtes $x_1, \ldots, x_q$ à $\mathcal{O}$. Si $\mathcal{O}$ se comporte comme E alors l'attaquant reçoit les valeurs $E(k, x_1), \ldots, E(k, x_q)$ pour k une clé uniformément aléatoire. Si $\mathcal{O}$ se comporte comme E^* alors l'attaquant reçoit les valeurs $\pi(x_1), \ldots, \pi(x_q)$ pour π une permutation uniformément aléatoire. Si E se comporte suffisamment comme E^*, il devrait être difficile de distinguer si $\mathcal{O}$ se comporte comme E ou comme E^*. C'est cette intuition que nous formalisons de la façon suivante : après avoir interagi avec l'oracle $\mathcal{O}$, l'attaquant $\mathcal{A}$ définit une valeur b à 0 ou 1. Intuitivement, c'est le choix qu'il fait sur la nature de $\mathcal{O}$ (il peut par exemple choisir de fixer b à 1 si il pense que $\mathcal{O}$ se comporte comme E et fixer b à 0 si il pense que $\mathcal{O}$ se comporte comme E^*). Si $\mathcal{O}$ se comporte comme E alors $\Pr\left[\mathcal{A}^{E_k(\cdot)} \Rightarrow 1\right]$ est la probabilité que l'attaquant définisse $b = 1$ pour une clé k uniformément aléatoire. Si $\mathcal{O}$ se comporte comme E^* alors $\Pr\left[\mathcal{A}^{E^*_\pi(\cdot)} \Rightarrow 1\right]$ est la probabilité que l'attaquant définisse $b = 1$ pour une permutation π uniformément aléatoire.

On définit l'avantage d'indistinguabilité de l'attaquant $\mathcal{A}$ comme étant la valeur :

$$\mathbf{Adv}_E(\mathcal{A}) = \left|\Pr\left[\mathcal{A}^{E_k(\cdot)} \Rightarrow 1\right] - \Pr\left[\mathcal{A}^{E^*_\pi(\cdot)} \Rightarrow 1\right]\right| \ .$$

On définit l'avantage d'indistinguabilité NCPA (pour Non Adaptative Chosen Plaintext Attack) comme étant la valeur :

$$\mathbf{Adv}^{\mathrm{ncpa}}_E(q) = \max_{\mathcal{A}} \mathbf{Adv}_E(\mathcal{A})$$

où le max est pris sur tous les attaquants faisant au plus q requêtes à $\mathcal{O}$ et de manière non-adaptative (les entrées $x_1, \ldots, x_q$ sont toutes choisies à l'avance, sans s'ajuster aux réponses de l'oracle $\mathcal{O}$).

On définit également l'avantage d'indistinguabilité CCA (pour Chosen-Ciphertext Attack) comme étant la valeur :

$$\mathbf{Adv}^{\mathrm{cca}}_E(q) = \max_{\mathcal{A}} \mathbf{Adv}_E(\mathcal{A})$$

où le max est pris sur tous les attaquants faisant au plus q requêtes, directes ou inverses à $\mathcal{O}$ (une requête inverse est une requête du type $\mathcal{O}^{-1}(y)$ égale à $E^{-1}(y,k)$ si $\mathcal{O}$ se comporte comme E et $\pi^{-1}(y)$ si $\mathcal{O}$ se comporte comme le schéma de chiffrement parfait), et de manière adaptative (les requêtes sont choisies au fur et à mesure des réponses données par l'oracle $\mathcal{O}$).

On effectue maintenant le lien entre avantage et distance statistique. Ceci est la première étape (parmi 6) de chacune des preuves de sécurité présentées dans cette thèse. Notre stratégie générale de preuves de sécurité par coupling est détaillée au chapitre 2.

1.3.3 Lien entre avantage et distance statistique (étape 1)

Soit Ω un espace de probabilité fini et μ et ν deux distributions de probabilités sur Ω. La distance statistique entre μ et ν est définie comme la valeur :

$$\|\mu - \nu\| = \frac{1}{2}\sum_{z\in\Omega} |\mu(z) - \nu(z)| = \sum_{\substack{z\in\Omega \\ \mu(z)\geq\nu(z)}} (\mu(z) - \nu(z)) \ .$$

Remarquons que la distance statistique est également égale à $\max_{S\subset\Omega}\{\mu(S) - \nu(S)\}$ où le max porte sur tous les sous-ensembles de Ω. L'avantage pour distinguer un schéma de chiffrement E donné et une permutation aléatoire peut être calculé en terme de distance statistique. En effet :

Lemme 1.1. *Soit $\mathcal{A}$ un attaquant NCPA souhaitant distinguer un schéma de chiffrement E donné d'une permutation aléatoire. Si l'oracle $\mathcal{O}$ est le schéma de chiffrement E, on note $\mu_{x_1,\ldots,x_q}$ la distribution des q sorties suite aux q requêtes $x_1,\ldots,x_q$ de l'attaquant (choisies deux à deux distinctes) et si l'oracle $\mathcal{O}$ est le schéma de chiffrement parfait E^*, on note $(\mu_0)_{x_1,\ldots,x_q}$ la distribution des q sorties suites aux q requêtes $x_1,\ldots,x_q$ de l'attaquant. L'avantage de l'attaquant $\mathcal{A}$ vérifie alors*

$$\mathbf{Adv}_E(q,\mathcal{A}) \leq \|\mu_{x_1,\ldots,x_q} - (\mu_0)_{x_1,\ldots,x_q}\| \ . \qquad \triangledown$$

Démonstration. Voir la technique des Coefficients H de Jacques Patarin [Pat91, Pat08].■

Ainsi, en prenant le maximum sur tous les attaquants $\mathcal{A}$, on obtient :

Lemme 1.2. *L'avantage NCPA d'indistinguabilité pour E vérifie :*

$$\mathbf{Adv}_E^{\mathrm{ncpa}}(q) \leq \max_{x_1,\ldots,x_q} \|\mu_{x_1,\ldots,x_q} - (\mu_0)_{x_1,\ldots,x_q}\| \ ,$$

où le max porte sur tous les $x_1,\ldots,x_q$ deux à deux distincts. $\triangledown$

Notons que $(\mu_0)_{x_1,\ldots,x_q}$ n'est autre que la distribution uniforme sur l'ensemble des $q-$uplets dont les coordonnées sont deux à deux distinctes. En effet, $E^*(\pi,\cdot)$, pour π une permutation uniformément aléatoire, n'est autre que π donc les sorties sont $\pi(x_1),\ldots,\pi(x_q)$ et sont donc uniformément aléatoires et deux à deux distinctes. Nous venons d'établir le lien entre la sécurité NCPA d'un schéma de chiffrement E et la distance statistique entre la distribution de probabilité des sorties (après q requêtes faites à E) et la distribution uniforme.

1.4 Preuves de sécurité dans les modèles idéalisés

En cryptographie, on cherche à concevoir des schémas qui vérifient certaines propriétés de sécurité. Par exemple, pour un schéma de chiffrement, on souhaite qu'il soit quasiment impossible de pouvoir déchiffrer des messages. La plupart du temps, pour s'assurer qu'un schéma est sécurisé, les cryptanalystes cherchent à attaquer le schéma pour mettre en défaut les propriétés de sécurité qu'on recherche. Si le schéma est faible, une attaque sera rapidement trouvée. Si aucune attaque n'est trouvée, le schéma peut être solide mais il n'y a aucune preuve. Une preuve mathématique serait nécessaire pour démontrer sa sécurité mais, la plupart du temps, il est bien trop difficile de prouver une borne inférieure de complexité en nombre de calculs pour une attaque. On procède alors à un compromis : on considère le même schéma où on a remplacé certains éléments internes par des éléments au comportement parfait. Par exemple, si le schéma utilise une permutation P suffisamment complexe, on va remplacer P par une permutation uniformément aléatoire. On peut autoriser (ou non) l'attaquant à faire des requêtes aux éléments idéalisés avec un accès en boîte noire. Ainsi, l'étude du nouveau schéma utilisant des éléments internes parfaits (accessibles en boîte noire) est plus simple à étudier et on peut obtenir une preuve mathématique de la sécurité de ce nouveau schéma. Bien sûr, cela ne donne pas une preuve de sécurité du schéma initial mais cela prouve que la structure est sûre et que toute attaque doit exploiter les propriétés des permutations et fonctions internes. Cette approche est également utilisée pour prouver la sécurité de schémas et protocoles utilisant des fonctions de hachage (par exemple le chiffrement OAEP ou les signatures FDH et PSS) en remplaçant les fonctions de hachage par des oracles aléatoires accessibles à l'attaquant, comme l'ont introduit Bellare et Rogaway [BR93].

Dans cette thèse, nous utiliserons des permutations aléatoires parfaites et des fonctions aléatoires parfaites. Nous prouverons que le schéma d'Even-Mansour itéré, le schéma de chiffrement par blocs paramétrable CLRW et le schéma de Feistel à clés alternées sont des schémas de chiffrement sûrs au sens où, si les permutations et fonctions internes utilisées sont parfaites, la structure des schémas ne permet pas de mettre en défaut les propriétés de sécurité recherchées. De plus, pour le cas du schéma CLRW, si le chiffrement par blocs idéal est remplacé par un chiffrement par blocs standard indistinguable du chiffrement par blocs idéal, alors le schéma entier reste sécurisé. Cette extension n'est pas présente pour le schéma d'Even-Mansour itéré et pour le schéma de Feistel à clés alternées.

Chapitre 2

Stratégie de preuve d'indistinguabilité par coupling

2.1 Coupling : définition et exemples

Le coupling est une technique probabiliste inventée par Wolfgang Doeblin à la fin des années 30. Elle consiste à corréler deux variables aléatoires afin de les comparer. Elle a été largement utilisée dans de nombreux domaines comme l'étude des marches aléatoires, des approximations de Poisson, des chaînes de Markov, des inégalités de corrélations, de la percolation, etc. Avant d'étudier plus précisément le coupling, nous présentons un exemple très simple qui permet de se forger une intuition sur cette technique.

2.1.1 Se forger une intuition sur le lancer de deux pièces

L'exemple suivant permet de développer l'intuition à propos du coupling, que nous définissons dans la section suivante. Soient deux pièces dont la première tombe sur `pile` avec probabilité 1/2 et la seconde tombe sur `pile` avec probabilité 3/5 (voir Figure 2.1).

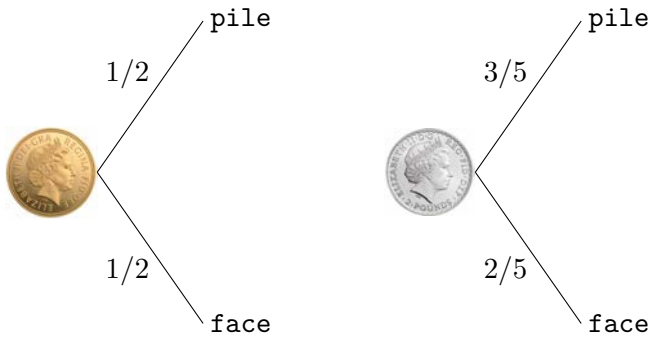

FIGURE 2.1 – Lancer de deux pièces

Pour cet exemple, la distance statistique entre la distribution du lancer de la première pièce et la distribution du lancer de la deuxième pièce est calculée très simplement : $\frac{1}{2}\left(\left|\frac{3}{5}-\frac{1}{2}\right|+\left|\frac{2}{5}-\frac{1}{2}\right|\right)=\frac{1}{10}$. Nous allons voir que nous pouvons retrouver cette distance statistique d'une autre façon. Considérons la situation où ces deux pièces sont très forte-

ment corrélées : quand la première tombe sur `pile`, la seconde tombe toujours sur `pile` et quand la première tombe sur `face`, la seconde tombe sur `pile` avec probabilité 1/5 (voir Figure 2.2).

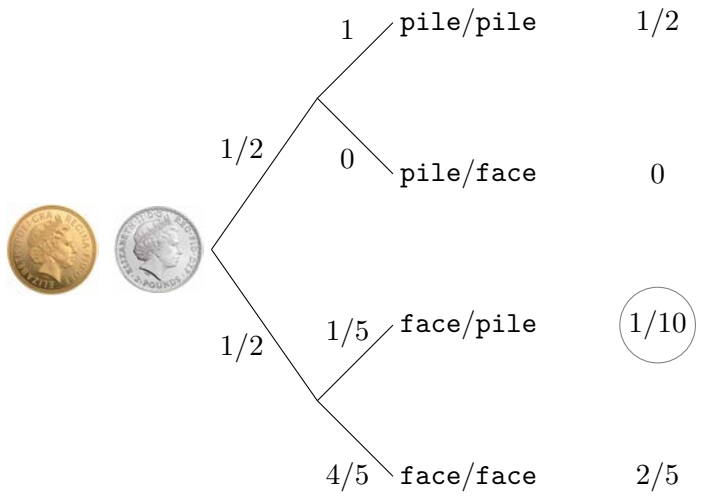

FIGURE 2.2 – Exemple de lancer de deux pièces avec forte corrélation

On retrouve bien les lois marginales de la première et de la seconde pièce puisque, par exemple, la seconde tombe sur `pile` avec probabilité $\frac{1}{2} + \frac{1}{2} \times \frac{1}{5} = \frac{3}{5}$. On remarque que les deux pièces tombent sur des faces différentes avec probabilité $0 + \frac{1}{10}$, c'est-à-dire exactement la distance statistique ! Ce n'est bien sûr pas une coïncidence et nous présentons dans la section suivante la théorie sous-jacente à cet exemple très simple.

2.1.2 Définition et lemme du coupling

Définition 2.1
Soit Ω un espace de probabilité fini et μ et ν deux distributions de probabilités sur Ω. Un coupling de μ et ν est une distribution de probabilité λ sur $\Omega \times \Omega$ telle que :

$$\forall x \in \Omega, \sum_{y \in \Omega} \lambda(x, y) = \mu(x) \text{ et } \forall y \in \Omega, \sum_{x \in \Omega} \lambda(x, y) = \nu(y).$$

Ainsi, λ est telle que μ et ν sont ses distributions marginales. ♦

Avant d'illustrer la technique par des exemples, nous présentons et démontrons le lemme du coupling qui représente l'utilité majeure du coupling et qui en fait sa force.

Lemme 2.1 (Lemme du coupling). *Soient μ et ν deux distributions sur Ω. Pour tout coupling λ de μ et ν et (X, Y) un couple de variables aléatoires de distribution λ, on a :*

$$\|\mu - \nu\| \leq \Pr[X \neq Y] \ . \qquad \triangledown$$

DÉMONSTRATION. Soit λ un coupling de μ et ν, et $(X, Y) \sim \lambda$, c'est-à-dire que, pour tout $x, y \in \Omega$, $\lambda(x, y) = \Pr[X = x \text{ et } Y = y]$, $\mu(x) = \Pr[X = x] = \sum_{z \in \Omega} \lambda(x, z)$ et $\nu(y) = \Pr[Y = y] = \sum_{z \in \Omega} \lambda(z, y)$. En particulier, pour tout $z \in \Omega$:

$$\lambda(z, z) = \Pr[X = z \text{ et } Y = z] \leq \min\{\Pr[X = z], \Pr[Y = z]\} \leq \min\{\mu(z), \nu(z)\} \ .$$

Ainsi :

$$\begin{aligned}
\Pr[X \neq Y] &= 1 - \Pr[X = Y] \\
&= 1 - \sum_{z \in \Omega} \Pr[X = z \text{ et } Y = z] \\
&= \sum_{z \in \Omega} \mu(z) - \sum_{z \in \Omega} \lambda(z, z) \\
&\geq \sum_{z \in \Omega} (\mu(z) - \min\{\mu(z), \nu(z)\}) \\
&= \sum_{\substack{z \in \Omega \\ \mu(z) \geq \nu(z)}} (\mu(z) - \nu(z)) \\
&= \|\mu - \nu\| \ .
\end{aligned}$$

■

Le lemme du coupling permet donc de majorer une distance statistique par la probabilité que deux variables aléatoires (non nécessairement indépendantes) soient différentes. Ce lemme est très pratique car le calcul d'une distance statistique peut être très compliqué et, pour X et Y astucieusement construits, il s'avère beaucoup plus simple de calculer la probabilité que ces deux variables aléatoires soient différentes.

Remarquons qu'on peut prouver qu'il existe toujours un coupling tel que l'inégalité du lemme précédent soit en fait une égalité pour ce coupling (voir [Lin92]). Nous n'avons pas besoin de ce résultat mais il est intéressant de noter que la technique du coupling, dans l'absolu, est optimale.

2.1.3 Exemples de coupling

Exemple 2.1. Considérons par exemple deux pièces P_1 et P_2 où P_1 est parfaitement équilibrée et P_2 tombe sur `pile` avec probabilité 3/4. Formellement, ces deux variables aléatoires ont chacune pour espace de probabilité $\Omega = \{\texttt{pile}, \texttt{face}\}$ et notons μ la distribution de P_1 et ν la distribution de P_2. Un coupling de μ et ν est une façon de corréler P_1 et P_2 dans l'espace de probabilité $\Omega \times \Omega$. Soit λ_1 le coupling de μ et ν défini par $\lambda_1(\texttt{x}, \texttt{y}) = \mu(\texttt{x}) \times \nu(\texttt{y})$ pour tout $(\texttt{x}, \texttt{y}) \in \Omega \times \Omega$. La distribution λ_1 correspond à la distribution du couple de pièces lorsque celles-ci sont totalement indépendantes. Soit λ_2 le coupling de μ et ν tel que $\lambda_2(\texttt{pile}, \texttt{pile}) = 1/2$ et $\lambda_2(\texttt{face}, \texttt{pile}) = \lambda_2(\texttt{face}, \texttt{face}) = 1/4$. La distribution λ_2 correspond à la distribution du couple de pièces lorsque les deux pièces sont maximalement corrélées. Par exemple, quand la première pièce tombe sur `pile`, la seconde tombe systématiquement sur `pile`. On représente ces couplings par les tableaux de probabilités suivants où la première colonne de chaque tableau liste les événements pour la première pièce et la première ligne liste les événements pour la seconde pièce.

λ_1	`pile`	`face`	
`pile`	3/8	1/8	=1/2
`face`	3/8	1/8	=1/2
	=3/4	=1/4	

λ_2	`pile`	`face`	
`pile`	1/2	0	=1/2
`face`	1/4	1/4	=1/2
	=3/4	=1/4	

TABLE 2.1 – Deux exemples de couplings de deux pièces

On remarque que, pour chaque coupling, les distributions marginales sont respectées car la somme de la première ligne est égale à 1/2, de la seconde à 1/2, de la 1ère colonne à 3/4 et de la 2ème colonne à 1/4.
Quelle est la distance statistique entre μ et ν ? On sait qu'elle est égale à la somme des $\mu(x) - \nu(x)$ sur les x tels que $\mu(x) \geq \nu(x)$ et donc la distance statistique est égale à $3/4 - 1/2 = 1/4$. On la trouve également dans le tableau définissant λ_2 en faisant la somme des éléments qui ne sont pas sur la diagonale $1/4 + 0$. Ainsi, λ_2 est un coupling qui correspond au cas d'égalité dans le lemme du coupling.
Dans la pratique, on va toujours chercher à construire le coupling qui corrèle le plus les deux variables aléatoires X et Y de telle façon que $\Pr[X \neq Y]$ soit minimale, pour obtenir la meilleure borne possible à $\|\mu - \nu\|$. ∗

Exemple 2.2. Considérons maintenant n pièces $P_1, \ldots, P_n$ tombant chacune sur `pile` avec probabilités $p_1, \ldots, p_n$ et n pièces $Q_1, \ldots, Q_n$ tombant chacune sur `pile` avec probabilités $q_1, \ldots, q_n$ tel que $p_i \leq q_i$ pour tout $i \leq n$. On souhaite prouver que, pour tout $k \in [0, n]$, la probabilité d'obtenir au moins k `pile` en lançant les n pièces $P_1, \ldots, P_n$ est inférieure ou égale à la probabilité d'obtenir au moins k `pile` en tirant les n pièces $Q_1, \ldots, Q_n$. Intuitivement, cela paraît évident mais pour le prouver, il semble nécessaire de s'engager dans des calculs longs et compliqués. Le coupling permet de dépasser ces difficultés techniques et de n'utiliser que l'argument à la base de notre intuition (le fait que les p_i sont inférieurs aux q_i). En effet, couplons les n pièces $P_1, \ldots, P_n$ avec les n pièces $Q_1, \ldots, Q_n$: pour tout $i \in [\![1, n]\!]$, définissons que, à chaque fois que P_i tombe sur `pile` alors Q_i tombe sur `pile` et à chaque fois que P_i tombe sur `face` alors Q_i tombe sur `pile` avec probabilité $(q_i - p_i)/(1 - p_i)$ et `face` sinon. On vérifie bien que les distributions marginales sont respectées car $p_i + (1 - p_i) \times (q_i - p_i)/(1 - p_i) = q_i$. Ayant couplé de cette manière, il est immédiat qu'à chaque fois que $P_1, \ldots, P_n$ produisent au moins k `pile` alors $Q_1, \ldots, Q_n$ produisent également au moins k `pile`, ce qui permet de conclure. On obtient également une majoration de la distance statistique entre la distribution des $P_1, \ldots, P_n$ et la distribution des $Q_1, \ldots, Q_n$. En effet :

$$\Pr[(P_1, \ldots, P_n) \neq (Q_1, \ldots, Q_n)] \leq \sum_{i=1}^{n} \Pr[P_i \neq Q_i] \leq \sum_{i=1}^{n} (q_i - p_i) \ .$$

Ainsi, le lemme du coupling nous permet de déduire que la distance statistique entre les deux distributions est majorée par $\sum_{i=1}^{n}(q_i - p_i)$. ∗

2.2 Diviser pour mieux régner (étape 2)

Considérons un schéma de chiffrement E dont nous cherchons à étudier l'indistinguabilité par rapport à une permutation aléatoire, dans le cadre d'un attaquant non-adaptatif qui fait des requêtes directes (attaques NCPA). Soient $x_1, \ldots, x_q$ les q requêtes de l'attaquant (choisies deux à deux distinctes) et notons μ_q la distribution des q sorties quand $x_1, \ldots, x_q$ sont envoyées à E et μ_0 la distribution des q sorties quand $x_1, \ldots, x_q$ sont envoyées à une permutation uniformément aléatoire. On remarque que μ_0 n'est autre que la distribution uniforme des $q-$uplets d'éléments deux à deux distincts puisque la permutation est uniformément aléatoire et les entrées deux à deux distinctes. Notre objectif est de majorer $\|\mu_q - \mu_0\|$.

Une nouvelle façon d'obtenir une distribution uniforme

Nous considérons une nouvelle façon d'obtenir la distribution uniforme : soient $u_1^0, \ldots, u_q^0$ tirés uniformément aléatoires et deux à deux distincts et f n'importe quelle permutation. Alors la distribution de $f(u_1^0), \ldots, f(u_q^0)$ est la distribution uniforme sur les $q-$uplets d'éléments deux à deux distincts. En particulier, pour n'importe quelle clé $k \in \mathcal{K}$, la distribution de $E(k, u_1^0), \ldots, E(k, u_q^0)$ est la distribution uniforme. On considère donc maintenant μ_0 comme la distribution des q sorties quand $u_1^0, \ldots, u_q^0$ sont envoyés à E.

Modifier progressivement les entrées

Grâce à cette nouvelle interprétation de μ_0, on observe que μ_q et μ_0 sont obtenus par le même procédé (le schéma de chiffrement E) mais pour des entrées différentes ($x_1, \ldots, x_q$ d'un côté et $u_1^0, \ldots, u_q^0$ de l'autre). Définissons, pour tout $\ell \in [\![0, q]\!]$: $u_{\ell+1}^\ell$ uniformément aléatoire dans $\{0,1\}^n \backslash \{x_1, \ldots, x_\ell\}$, $u_{\ell+2}^\ell$ uniformément aléatoire dans $\{0,1\}^n \backslash \{x_1, \ldots, x_\ell, u_{\ell+1}^\ell\}$ et ainsi de suite pour $u_{\ell+3}^\ell, \ldots, u_q^\ell$. On considère alors la distribution μ_ℓ des q sorties quand $x_1, \ldots, x_\ell, u_{\ell+1}^\ell, \ldots, u_q^\ell$ sont envoyés à E. Pour étudier $\|\mu_q - \mu_0\|$, nous allons étudier $\|\mu_{\ell+1} - \mu_\ell\|$ pour tout $\ell \in [\![0, q-1]\!]$ ce qui nous permettra de conclure grâce à l'inégalité triangulaire :

$$\|\mu_q - \mu_0\| \leq \sum_{\ell=0}^{q-1} \|\mu_{\ell+1} - \mu_\ell\| \ . \tag{2.1}$$

Pour un ℓ fixé, la distribution $\mu_{\ell+1}$ correspond à la distribution obtenue avec les entrées $x_1, \ldots, x_\ell, x_{\ell+1}, u_{\ell+2}^{\ell+1}, \ldots, u_q^{\ell+1}$ et μ_ℓ avec les entrées $x_1, \ldots, x_\ell, u_{\ell+1}^\ell, \ldots, u_q^\ell$. On remarque que toutes les entrées sont uniformément aléatoires à partir du rang $\ell+2$, on peut donc se douter que ces entrées n'ont pas d'incidence sur le calcul de $\|\mu_{\ell+1} - \mu_\ell\|$. En effet, soit $\nu_{\ell+1}$ la distribution des $\ell+1$ sorties obtenues avec les entrées $x_1, \ldots, x_{\ell+1}$ et ν_ℓ la distribution des $\ell+1$ sorties obtenues avec les entrées $x_1, \ldots, x_\ell, u_{\ell+1}^\ell$, alors

$$\|\mu_{\ell+1} - \mu_\ell\| = \|\nu_{\ell+1} - \nu_\ell\| \ .$$

La preuve, assez technique, est en appendice de notre article [LS14].

2.3 Coupler les deux distributions adjacentes (étape 3)

Pour un ℓ fixé, il s'agit maintenant de construire un coupling de $\nu_{\ell+1}$ et ν_ℓ. Cette construction est propre à chaque schéma de chiffrement qu'on étudie. Les trois premiers articles présentés dans cette thèse montrent en détails comment définir le coupling suivant le schéma étudié.

2.4 Majorer la probabilité de ne pas coupler (étape 4)

Le lemme du coupling (lemme 2.1) nous permet de majorer la distance statistique entre $\nu_{\ell+1}$ et ν_ℓ à l'aide du coupling. Si X et Y sont les deux variables aléatoires couplées ayant respectivement pour distributions $\nu_{\ell+1}$ et ν_ℓ, il s'agit alors de majorer la probabilité que $X \neq Y$. Cette étape est, là aussi, propre au schéma étudié et c'est ici qu'interviennent presque systématiquement des calculs de collisions.

2.5 En déduire un majorant de l'avantage NCPA (étape 5)

Cette étape utilise l'argument de l'étape 1 et nous aurions pu unir ces 2 étapes mais nous préférons les dissocier pour présenter plus explicitement le cheminement mental de cette stratégie. L'étape 1 consiste à translater le calcul d'avantage à un calcul de distance statistique. L'étape 5 consiste très simplement à faire le chemin inverse, en utilisant le même lemme 1.2 qui majore l'avantage NCPA pour distinguer deux distributions par la distance statistique qui les sépare.

2.6 Doubler le nombre de tours pour obtenir une sécurité CCA à partir d'une sécurité NCPA (étape 6)

La technique du coupling est adaptée pour étudier la sécurité NCPA d'un schéma car, les requêtes étant choisies par avance, la probabilité de coupler peut, plus ou moins facilement, être calculée. En revanche, pour une attaque adaptative, les requêtes sont choisies au fur et à mesure des réponses de l'oracle et le calcul de la probabilité de coupler est alors, à l'heure actuelle, très difficile, car toutes les requêtes qui suivent x_1 sont conditionnées par les réponses de l'oracle, modifiant ainsi l'uniformité de l'aléa de l'espace de probabilité considéré. Le coupling est, en soit, possible (quelles que soient deux variables X et Y dans le même espace de probabilité, il existe toujours un coupling optimal de ces deux variables tel que l'inégalité du lemme 2.1 soit une égalité, c'est-à-dire que la probabilité que les deux variables couplées soient différentes est égale à la distance statistique entre les distributions de X et Y) mais le conditionnement des requêtes de l'attaquant rend très difficile le calcul de la probabilité de coupler. Pour pallier ce problème, on utilise deux techniques :

Théorème 2.2 (Sécurité CCA par coefficients H). *Soient E_1 et E_2 deux schémas de chiffrements, dépendant éventuellement d'oracles extérieurs, vérifiant :*

$$\mathbf{Adv}^{\mathrm{ncpa}}_{E_1} \leq \beta_1 \text{ et } \mathbf{Adv}^{\mathrm{ncpa}}_{E_2} \leq \beta_2,$$

pour deux réels $\beta_1, \beta_2 \in [0,1]$. Alors :

$$\mathbf{Adv}^{\mathrm{cca}}_{E_2^{-1} \circ E_1} \leq 2(\sqrt{\beta_1} + \sqrt{\beta_2}) \ . \qquad \diamondsuit$$

Nous prouvons ce théorème dans les chapitres 3, 4 et 5 avec les notations et dans le contexte du schéma d'Even-Mansour, du schéma CLRW et du schéma KAF, respectivement.

Il existe un théorème plus puissant mais qui ne s'applique qu'au cas des schémas de chiffrement qui ne dépendent pas d'oracles extérieurs. Dans la pratique, nous n'avons pas réussi à transposer ce théorème au cas des schémas d'Even-Mansour, des tweakable blockciphers et des key-alternating feistel ciphers mais il est probable que ce théorème soit effectivement transposable à des chiffrements dépendant d'oracles extérieurs.

Théorème 2.3 (Maurer-Renner-Pietrzak [MPR07],Cogliati-Patarin-Seurin [CPS14]). *Soient E_1 et E_2 deux schémas de chiffrements ne dépendant pas d'oracles extérieurs et vérifiant :*

$$\mathbf{Adv}^{\mathrm{ncpa}}_{E_1} \leq \beta_1 \text{ et } \mathbf{Adv}^{\mathrm{ncpa}}_{E_2} \leq \beta_2,$$

pour deux réels $\beta_1, \beta_2 \in [0,1]$. *Alors :*

$$\mathbf{Adv}^{\mathrm{cca}}_{E_2^{-1} \circ E_1} \leq \beta_1 + \beta_2 \ . \qquad \diamondsuit$$

Démonstration. Voir [MPR07] pour une preuve dans le cadre de la théorie des « Random Systems » et [CPS14] pour une preuve, beaucoup plus simple, dans le cadre de la théorie des Coefficients H. ■

2.7 Stratégie de preuve d'indistinguabilité par coupling

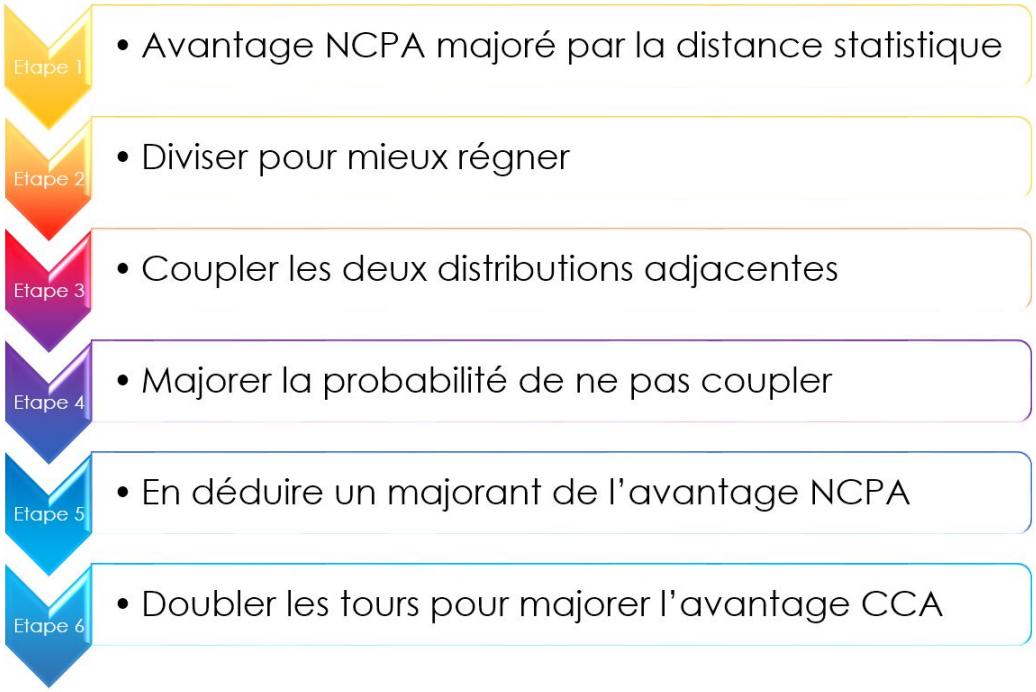

Figure 2.3 – Stratégie de preuve d'indistinguabilité par coupling

Cette stratégie, en 6 étapes que nous venons de présenter dans la section précédente, est résumée dans la Figure 2.3. Pour chacun de nos articles [LPS12] [LS13b] [LS14], nous avons appliqué cette stratégie en l'ajustant au schéma étudié. Les étapes 1, 2 et 5 ne nécessitent pas d'ajustement selon le schéma, elles sont assez génériques. Les étapes 3 et 4 sont les plus importantes et il s'agit de définir un coupling pour le schéma donné et calculer les probabilités de ne pas coupler. L'étape 6 nécessite un ajustement au schéma étudié. Pour le schéma d'Even-Mansour itéré [LPS12], le schéma de chiffrement paramétrable CLRW [LS13b] et le schéma de Feistel à clés-alternées [LS14], nous avons utilisé la technique des Coefficients H pour obtenir la sécurité CCA en fonction de la sécurité NCPA.

Cette stratégie de preuve par coupling a été utilisée en particulier par Morris *et al.* [MRS09] pour l'analyse des schémas de Feistel maximalement non-balancés, Hoang et

Rogaway [HR10] pour l'analyse des schémas de Feistel balancés, non-balancés et généralisés. Nos travaux sont fortement inspirés de ces deux articles fondateurs. Nos résultats [LPS12, LS13b, LS14] sont « simplement » l'application de cette stratégie à d'autres schémas, en prenant en compte la dépendance par rapport à des oracles extérieurs.

Chapitre 3

Preuve d'indistinguabilité du schéma d'Even-Mansour itéré

Dans ce chapitre, on présente le schéma d'Even-Mansour itéré et nous prouvons son indistinguabilité face à une attaque CCA jusqu'à un nombre de requêtes en $\mathcal{O}(N^{\frac{t}{t+2}})$ pour un nombre pair de tours t. Cette preuve utilise le coupling et suit la méthode que nous avons présenté dans le chapitre 2.

3.1 Le schéma d'Even-Mansour itéré

Le schéma d'Even-Mansour

Even et Mansour [EM97] ont proposé en 1997 le schéma de chiffrement suivant : étant donné une permutation publique P sur $\mathcal{I}_n$ (par exemple AES-128 avec une clé publique fixée) et deux clés secrètes k_0 et k_1, on note $\mathtt{EM}_{P,(k_0,k_1)}$ (voir Figure 3.1) le schéma d'Even-Mansour défini par :

$$\forall x \in \mathcal{I}_n, \mathtt{EM}_{P,(k_0,k_1)}(x) := k_1 \oplus P(k_0 \oplus x) \ .$$

Cette idée provient de l'observation du design de DESX, proposé par Rivest en 1984 (non publié) et formalisé par Killian et Rogaway [KR01], un schéma qui renforce le DES en xorant une clé aléatoire k_0 en entrée du DES et une clé aléatoire k_1 en sortie du DES (augmentant ainsi la taille des clés de 56 à 184 bits).

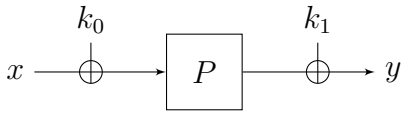

FIGURE 3.1 – Le schéma d'Even-Mansour.

Généralisation : le schéma d'Even-Mansour itéré

En 2012, le schéma d'Even-Mansour a été généralisé à plusieurs tours par Bogdanov *et al.* [BKL+12] : étant donné $\boldsymbol{P}$ un $t-$uplet de permutations aléatoires publiques $(P_1, \ldots, P_t)$

sur $\mathcal{I}_n$ et k un $(t+1)-$uplet de clés secrètes $(k_0, \ldots, k_t)$, on note $\mathtt{EM}_{\boldsymbol{P},k}$ (voir Figure 3.2) le schéma d'Even-Mansour itéré défini par :

$$\forall x \in \mathcal{I}_n, \mathtt{EM}_{\boldsymbol{P},k} := k_t \oplus P_t(k_{t-1} \oplus P_{t-1}(\cdots P_1(k_0 \oplus x)\cdots)) \ .$$

Par la suite, pour $t = 1$, on parlera du schéma d'Even-Mansour et pour $t \geq 2$, on parlera du schéma d'Even-Mansour itéré.

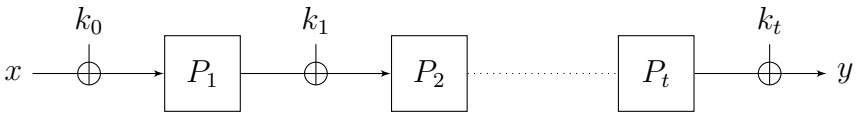

FIGURE 3.2 – Le schéma d'Even-Mansour itéré.

3.2 Les preuves de sécurité du schéma d'Even-Mansour itéré

Dans leur article fondateur, Even et Mansour [EM97] se sont placés dans le modèle de la permutation aléatoire (comme nous l'avons présenté en section 1.4), c'est-à-dire en remplaçant P par un oracle implémentant une permutation uniformément aléatoire publique (l'attaquant peut faire des requêtes à P et à P^{-1}). Dans ce cas là, avec P, k_0, k_1 uniformément aléatoires, si q_p est le nombre de requêtes de l'attaquant à P ou P^{-1}, q_e le nombre de requêtes de l'attaquant à $\mathtt{EM}_{P,(k_0,k_1)}$ ou $\mathtt{EM}^{-1}_{P,(k_0,k_1)}$ (une attaque CCA) et $N = 2^n$ le nombre d'éléments de $\mathcal{I}_n$, alors Even et Mansour ont prouvé qu'un attaquant peut déchiffrer un chiffré y avec probabilité $\mathcal{O}\left(\frac{q_e q_p}{N}\right)$ (en excluant, bien sûr, le cas où y a déjà été déchiffré par une requête de l'attaquant parmi les q_e requêtes). En fait, le schéma d'Even-Mansour $\mathtt{EM}_{P,(k_0,k_1)}$, pour P, k_0, k_1 uniformément aléatoires, est indistinguable d'une permutation uniformément aléatoire π si $q_e, q_p \ll N^{1/2}$ face à une attaque CCA (voir section 3.5.1).

Dans leur article généralisant le schéma d'Even-Mansour à plusieurs tours, Bogdanov *et al.* [BKL$^+$12] ont prouvé que, pour $t \geq 2$, le schéma est indistinguable d'une permutation aléatoire pour des nombres de requêtes vérifiant $q_e, q_{P_1}, \ldots, q_{P_t} \ll N^{2/3}$ face à une attaque CCA. Ils ont également présenté une attaque nécessitant $\Omega(N^{t/(t+1)})$ requêtes ce qui prouve que leur borne de sécurité est optimale pour $t = 2$, et ont conjecturé que leur attaque en $\Omega(N^{t/(t+1)})$ requêtes est optimale. Il restait donc, en 2012, à améliorer, si possible, la preuve de sécurité pour $t \geq 3$.

En Aout 2012, John Steinberger [Ste12] découvre une nouvelle façon de prouver la sécurité du schéma d'Even-Mansour itéré à $t \geq 3$ tours à l'aide de la distance d'Hellinger. Cette découverte lui permet de prouver l'indistinguabilité du schéma d'Even-Mansour itéré à $t \geq 3$ tours jusqu'à $\mathcal{O}(N^{3/4})$ requêtes, ce qui donne une preuve de sécurité optimale pour $t = 3$.

Nous avons présenté à ASIACRYPT 2012 (Lampe, Patarin, Seurin [LPS12]) une preuve d'indistinguabilité du schéma d'Even-Mansour itéré à t tours pour $q_e, q_{P_1}, \ldots, q_{P_t}$ requêtes si $q_e, q_{P_1}, \ldots, q_{P_t} \ll N^{\frac{t}{t+1}}$ pour une attaque NCPA et, pour t pair, une preuve d'indistinguabilité si $q_e, q_{P_1}, \ldots, q_{P_t} \ll N^{\frac{t}{t+2}}$ pour une attaque CCA (si t est impair, on a la même borne que pour $t-1$). Étant donné l'attaque de Bogdanov *et al.* [BKL$^+$12] en $\Omega(N^{t/(t+1)})$ requêtes, notre preuve est optimale pour une attaque NCPA (pour toutes valeurs de $t \geq 1$) et asymptotiquement optimale pour une attaque CCA. La technique du

t	[BKL$^+$12]	[Ste12]	[LPS12]	[CS14]
2	2/3	2/3	1/2	2/3
3	2/3	3/4	1/2	3/4
4	2/3	3/4	2/3	4/5
5	2/3	3/4	2/3	5/6
6	2/3	3/4	3/4	6/7
7	2/3	3/4	3/4	7/8
8	2/3	3/4	4/5	8/9

TABLE 3.1 – Amélioration des bornes de sécurité CCA pour les premières valeurs de t de 1 à 8. Chaque valeur correspond à l'exposant e pour une borne de sécurité en $\mathcal{O}(N^e)$.

coupling utilisée dans cette preuve permet, pour la première fois, d'obtenir une borne de sécurité qui augmente avec le nombre de tours t. Cette borne de sécurité en $\Omega(N^{\frac{t}{t+2}})$ tend asymptotiquement vers la borne optimale en $\Omega(N^{\frac{t}{t+1}})$.

En 2014, Chen et Steinberger [CS14] ont prouvé la conjecture émise par Bogdanov et al. [BKL$^+$12] en donnant une preuve de sécurité optimale du schéma d'Even-Mansour à t tours qui coïncide avec la complexité de l'attaque en $N^{\frac{t}{t+1}}$ requêtes pour une attaque CCA. Leur preuve de sécurité utilise la technique des coefficients H de Jacques Patarin [Pat91, Pat08] et repose sur un calcul très précis et très complexe de la probabilité de connecter un $q-$uplet d'entrées arbitraires à un $q-$uplet de sorties arbitraires.

Nous présentons l'amélioration des bornes de sécurité CCA pour les premiers valeurs de t de 1 à 8 dans la table 3.1. Remarquons que nous n'améliorons la borne de sécurité par rapport à [BKL$^+$12] et [Ste12] qu'à partir de 8 tours. La dernière colonne correspond à la borne optimale obtenue par [CS14].

3.3 Travaux connexes

Attaques

On s'intéresse dans cette thèse aux preuves de sécurité mais il est important de noter que le schéma d'Even-Mansour a également été étudié sous le point de vue des attaques, principalement pour récupérer la clé secrète. Daemen [Dae91] a présenté une attaque sur le schéma d'Even-Mansour nécessitant q_p requêtes directes choisies à P et q_e requêtes choisies à E avec $q_p q_e = \Omega(N)$. La complexité de son attaque est donc minimale pour $q_e = q_p = \Omega(N^{1/2})$. En 2000, Biryukov et Wagner [BW00] ont présenté une attaque nécessitant $\Omega(N^{1/2})$ requêtes à P et à E sans avoir besoin de choisir les requêtes (known plaintext attack). Néanmoins, cette attaque ne permet pas de compromis entre le nombre de requêtes à P et le nombre de requêtes à E comme le permet l'attaque de Daemen. Plus récemment, en 2012, Dunkelman, Keller et Shamir [DKS12] ont amélioré l'attaque de [BW00] en permettant un tel compromis entre les requêtes à P et les requêtes à E, rendant l'attaque optimale.

Le schéma d'Even-Mansour à 1 tour a également été attaqué dans le cas d'une attaque impliquant plusieurs utilisateurs (Fouque, Joux et Mavromati [FJM13]), permettant ainsi

d'amortir le coup d'une attaque à $N^{1/3}$ requêtes par utilisateur.

Variantes du schéma d'Even-Mansour

En 2004, Gentry et Ramzan [GR04] ont prouvé que le schéma d'Even-Mansour reste sûr si l'on remplace la permutation P par un schéma de Feistel à 4 tours, où les fonctions de tours sont des oracles implémentant des fonctions aléatoires publiques. Dans cette thèse, nous présentons au chapitre 5 une variante proche de celle de [GR04] qui consiste à remplacer, dans un schéma d'Even-Mansour itéré à t tours, les permutations P_i par des schémas de Feistel à 2 tours.

Minimalisme

Il est légitime de s'intéresser au minimalisme du schéma d'Even-Mansour et du schéma d'Even-Mansour itéré. Dunkelman, Keller et Shamir [DKS12] ont prouvé que le schéma d'Even-Mansour à 1 tour n'est pas minimal et qu'en posant $k_1 = k_0$ on obtient un schéma avec deux fois moins de clés et une sécurité équivalente et optimale pour cette taille de clé. Un an plus tard, Dinur, Dunkelman, Keller et Shamir [DDKS13] présentent une attaque sur le schéma d'Even-Mansour à 3 tours et une clé ($k_3 = k_2 = k_1 = k_0$) en $o(N)$ au lieu de $O(N)$ pour une recherche exhaustive. A l'heure actuelle, l'étude de certaines minimisations du schéma d'Even-Mansour (prendre des clés égales, ou des permutations égales par exemple) est en cours. Nous présentons au chapitre 6 une preuve de sécurité pour le schéma d'Even-Mansour à 2 tours pour certaines minimisations (Chen, Lampe, Lee, Seurin, Steinberger [CLL+14]).

3.4 Indistinguabilité du schéma d'Even-Mansour itéré face à une attaque NCPA

On s'intéresse ici à la sécurité du schéma d'Even-Mansour itéré face à une attaque NCPA. Étant donné que les permutations internes et la permutation externe sont publiques, on peut se demander comment on définit une attaque NCPA dans ce cas. Nous présenterons ici un modèle de distingueur NCPA assez restreint qui nous permettra, par la suite, de prouver la sécurité CCA sans restriction. Cette preuve face à une attaque NCPA doit être considérée comme une étape vers la preuve face à une attaque CCA.

3.4.1 Notations

Pour des entiers $n, q, q_1, \ldots, q_t \in \mathbb{N}^\times$, on note :
- $(\mathcal{I}_n)^{*q}$ l'ensemble des $(x^1, \ldots, x^q) \in \mathcal{I}_n$ tels que $x^i \neq x^j$ pour tout $i \neq j$,
- $(\mathcal{I}_n)^{*q_1,\ldots,q_t}$ l'ensemble $(\mathcal{I}_n)^{*q_1} \times \cdots \times (\mathcal{I}_n)^{*q_t}$,
- $(N)_q = N(N-1)\cdots(N-q+1)$.

Remarquons que $|(\mathcal{I}_n)^{*q}| = (N)_q$. Etant donné $P \in \mathcal{P}_n$ et $x = (x^1, \ldots, x^q) \in (\mathcal{I}_n)^{*q}, y = (y^1, \ldots, y^q) \in (\mathcal{I}_n)^{*q}$, on écrira $P(x) = y$ pour signifier que $P(x^i) = y^i$ pour tout $i = 1, \ldots, q$. Etant donné $\boldsymbol{P} = (P_1, \ldots, P_t) \in (\mathcal{P}_n)^t$ et $a = (a_1, \ldots, a_t), b = (b_1, \ldots, b_t) \in (\mathcal{I}_n)^{*q_1,\ldots,q_t}$, avec $a_i = (a_i^1, \ldots, a_i^{q_i})$ et $b_i = (b_i^1, \ldots, b_i^{q_i})$ pour tout $i = 1, \ldots, t$, on écrira $\boldsymbol{P}(a) = b$ pour signifier que $P_i(a_i) = b_i$ pour $i = 1, \ldots, t$ (*i.e.* $P_i(a_i^j) = b_i^j$ pour $j = 1, \ldots, q_i$).

Étant donné $k \in \mathcal{I}_n$, on note $\oplus_k$ l'application $x \mapsto x \oplus k$ de $\mathcal{I}_n$ dans $\mathcal{I}_n$. On note Ω_t l'ensemble $(\mathcal{P}_n)^t \times (\mathcal{I}_n)^{t+1}$. Ainsi, un schéma d'Even-Mansour itéré $\mathtt{EM}_{\boldsymbol{P},k}$ avec $(\boldsymbol{P}, k) = (P_1, \ldots, P_t, k_0, \ldots, k_t) \in \Omega_t$ peut s'écrire :

$$\mathtt{EM}_{\boldsymbol{P},k} = \oplus_{k_t} \circ P_t \circ \oplus_{k_{t-1}} \circ \cdots \circ \oplus_{k_1} \circ P_1 \circ \oplus_{k_0} \ .$$

3.4.2 Distingueurs NCPA

Dans le schéma d'Even-Mansour itéré, les permutations internes $P_1, \ldots, P_t$ sont considérées publiques. Ainsi, dans la définition d'un distingueur, on doit considérer ces accès aux permutations internes. On considère donc des distingueurs qui interagissent avec un système de $t+1$ permutations. L'objectif du distingueur est de savoir si il interagit avec le système dit « idéal » de $t+1$ permutations uniformément aléatoires et indépendantes (qu'on notera UAI par la suite) $(P_1, \ldots, P_t, Q)$ ou si il interagit avec le système dit « réel » de $t+1$ permutations $(P_1, \ldots, P_t, \mathtt{EM}_{\boldsymbol{P},k})$ où $P_1, \ldots, P_t$ sont UAI et $\mathtt{EM}_{\boldsymbol{P},k}$ est le schéma d'Even-Mansour itéré associé à $\boldsymbol{P} = (P_1, \ldots, P_t)$ et $k = (k_0, \ldots, k_t)$. On appellera les t permutations $P_1, \ldots, P_t$ les permutations « internes » et la dernière permutation (Q ou $\mathtt{EM}_{\boldsymbol{P},k}$) la permutation « externe ». Un $(q_1, \ldots, q_t, q_e)-$distingueur est un distingueur qui fait au plus q_i requêtes à P_i pour $i = 1, \ldots, t$ et q_e requêtes à la permutation externe. Nous considérons les distingueurs avec une capacité de calcul non bornée. Comme d'habitude pour ce genre de preuves et de distingueurs, on se limite, sans perte de généralité, aux distingueurs déterministes qui ne font pas de requêtes redondantes et qui font toujours le nombre maximal de requêtes autorisées à chaque permutation. Une requête sera définie comme un triplet (i, b, z) où $i \in [1; t+1]$ correspond à la permutation qui fait l'objet de la requête, b est un bit qui correspond au sens de la requête ($b = 0$ pour une requête directe et $b = 1$ pour une requête inverse) et $z \in \mathcal{I}_n$ est la valeur envoyée à la permutation. Dans cette section, on considère uniquement les distingueurs NCPA qu'on définit par :

Définition 3.1 (Distingueur NCPA)
Un $(q_1, \ldots, q_t, q_e)-$distingueur NCPA $\mathcal{D}$ agit en deux étapes :

1. Dans un premier temps, le distingueur $\mathcal{D}$ ne fait des requêtes qu'aux permutations internes $(P_1, \ldots, P_t)$. Ces requêtes peuvent être adaptatives et directes ou inverses. Durant cette étape, il fait exactement q_i requêtes à P_i pour $i = 1, \ldots, t$.
2. Dans un second temps, le distingueur $\mathcal{D}$ choisit un q_e-uplet de requêtes $(x^1, \ldots, x^{q_e})$ qu'il envoie à la permutation externe du système et reçoit les réponses $(y^1, \ldots, y^{q_e})$. Ces requêtes sont donc directes et non-adaptatives. ♦

Remarquons que cette définition du distingueur est assez restrictive : l'attaquant ne peut faire ses requêtes à la permutation externe qu'après avoir fait ses requêtes aux permutations internes. Cette restriction ne reflète pas la réalité d'une attaque NCPA qui, de manière générale, n'impose pas d'ordre dans les requêtes. Cette restriction est artificielle et doit être vue comme une première étape pour obtenir la sécurité CCA. Notre preuve de sécurité pour un distingueur NCPA comme nous l'avons défini (restreint) peut s'étendre à un distingueur NCPA non-restreint sur l'ordre mais nous préférons prouver ce résultat plus faible et plus simple qui nous permet, malgré la restriction, d'obtenir la sécurité CCA par la suite.

La probabilité d'un évènement *event* quand $\mathcal{D}$ interagit avec le système idéal ($P_1, \ldots, P_t, Q$ permutations UAI) sera notée $\Pr^*[event]$ tandis qu'elle sera notée $\Pr[event]$ dans le

cas où $\mathcal{D}$ interagit avec le système réel $(P_1, \ldots, P_t, \mathtt{EM}_{P,k}$ avec $P_1, \ldots, P_t$ des permutations UAI et k uniformément aléatoire dans $\mathcal{I}_n^{t+1})$. Avec ces notations, l'avantage d'un distingueur $\mathcal{D}$ est défini comme $|\Pr[\mathcal{D}(1^n) = 1] - \Pr^*[\mathcal{D}(1^n) = 1]|$ (on ne note pas les appels aux oracles qui se déduisent des notations $\Pr[\cdot]$ et $\Pr^*[\cdot]$). L'avantage maximal d'un $(q_1, \ldots, q_t, q_e)-$distingueur ATK (où ATK est NCPA ou CCA) contre un schéma d'Even-Mansour itéré à t tours sera noté $\mathbf{Adv}^{\mathrm{atk}}_{\mathcal{EM}[t]}(q_1, \ldots, q_t, q_e)$. Quand le nombre total de requêtes est égal à q, on notera simplement $\mathbf{Adv}^{\mathrm{atk}}_{\mathcal{EM}[t]}(q)$.

3.4.3 Lien entre distance statistique et avantage (étape 1)

On sait déjà que, pour n'importe quel schéma de chiffement E, l'avantage NCPA pour distinguer E d'une permutation aléatoire est majoré par la valeur maximale, sur les entrées $x_1, \ldots, x_q$, de la distance statistique entre la distribution des sorties $(E_k(x_1), \ldots, E_k(x_q))$, pour k uniformément aléatoire, et la distribution uniforme sur $(\mathcal{I}_n)^{*q}$ (voir Lemme 1.2). La particularité du schéma d'Even-Mansour est qu'il y a des permutations internes à considérer. Ici, la principale tâche est donc de majorer la distance statistique de la distribution des sorties du schéma d'Even-Mansour itéré *conditionnée par l'information partielle sur les permutations internes* (c'est-à-dire, la condition $\boldsymbol{P}(a) = b$ pour $a, b \in (\mathcal{I}_n)^{*q_1,\ldots,q_t}$) et la distribution uniforme sur $(\mathcal{I}_n)^{*q_e}$. Pour se faire, on introduit la définition suivante :

Définition 3.2
Soient $q_1, \ldots, q_t, q_e$ des entiers positifs, $a, b \in (\mathcal{I}_n)^{*q_1,\ldots,q_t}$ et $x \in (\mathcal{I}_n)^{*q_e}$. On note $\mu_x(\cdot|\boldsymbol{P}(a) = b)$ la distribution de $\mathtt{EM}_{\boldsymbol{P},k}(x)$ conditionnée sur l'événement $\boldsymbol{P}(a) = b$ (*i.e.* la clé $k = (k_0, \ldots, k_t)$ est uniformément aléatoire et les permutations $\boldsymbol{P} = (P_1, \ldots, P_t)$ sont UAI et vérifient $\boldsymbol{P}(a) = b$). On note également $\mu^*_{q_e} = 1/(N)_{q_e}$ la distribution uniforme sur $(\mathcal{I}_n)^{*q_e}$. ♦

On a alors l'expression suivante pour $\mu_x(\cdot|\boldsymbol{P}(a) = b)$:

Lemme 3.1. *Soient $a, b \in (\mathcal{I}_n)^{*q_1,\ldots,q_t}$ et $x \in (\mathcal{I}_n)^{*q_e}$. Alors, pour tout $y \in (\mathcal{I}_n)^{*q_e}$, on a :*

$$\mu_x(y|\boldsymbol{P}(a) = b) = \frac{\#\{(\boldsymbol{P}, k) \in \Omega_t : \mathtt{EM}_{\boldsymbol{P},k}(x) = y \wedge \boldsymbol{P}(a) = b\}}{|\Omega_t| / \prod_{i=1}^{t} (N)_{q_i}} \ . \qquad \triangledown$$

Démonstration. On sait que le nombre de $(\boldsymbol{P}, k) \in \Omega_t$ tels que $\boldsymbol{P}(a) = b$ est égal à $|\Omega_t| / \prod_{i=1}^{t} (N)_{q_i}$ donc la formule de Bayes donne :

$$\begin{aligned}
\mu_x(y|\boldsymbol{P}(a) = b) &= \Pr[\mathtt{EM}_{\boldsymbol{P},k}(x) = y | \boldsymbol{P}(a) = b] \\
&= \frac{\Pr[\mathtt{EM}_{\boldsymbol{P},k}(x) = y \wedge \boldsymbol{P}(a) = b]}{\Pr[\boldsymbol{P}(a) = b]} \\
&= \frac{\#\{(\boldsymbol{P}, k) \in \Omega_t : \mathtt{EM}_{\boldsymbol{P},k}(x) = y \wedge \boldsymbol{P}(a) = b\}}{\#\{(\boldsymbol{P}, k) \in \Omega_t : \boldsymbol{P}(a) = b\}} \\
&= \frac{\#\{(\boldsymbol{P}, k) \in \Omega_t : \mathtt{EM}_{\boldsymbol{P},k}(x) = y \wedge \boldsymbol{P}(a) = b\}}{|\Omega_t| / \prod_{i=1}^{t} (N)_{q_i}} \ .
\end{aligned}$$ ■

Le lemme suivant établit la relation entre l'avantage d'un distingueur NCPA et la distance statistique entre $\mu_x(\cdot|\boldsymbol{P}(a) = b)$ et $\mu^*_{q_e}$. On obtient le même résultat qu'au Lemme 1.2 pour un schéma de chiffrement classique avec la particularité, ici, qu'on prenne en compte le conditionnement sur les équations sur les permutations internes. Ce résultat correspond à l'étape 1 dans notre stratégie de preuve par coupling présentée au chapitre 2.

Lemme 3.2. *Soient $q_1, \ldots, q_t, q_e$ des entiers positifs. Soit α un réel positif tel que, pour tous $a, b \in (\mathcal{I}_n)^{*q_1,\ldots,q_t}$ et $x \in (\mathcal{I}_n)^{*q_e}$, on a :*

$$\|\mu_x(\cdot|\boldsymbol{P}(a) = b) - \mu^*_{q_e}\| \leq \alpha \ .$$

Alors $\mathbf{Adv}^{\text{ncpa}}_{\mathcal{EM}[t]}(q_1, \ldots, q_t, q_e) \leq \alpha$. ▽

Démonstration. Fixons un $(q_1, \ldots, q_t, q_e)$-distingueur NCPA $\mathcal{D}$. Un tel distingueur fait d'abord ses requêtes aux permutations internes $(P_1, \ldots, P_t)$. Soit τ la transcription de l'interaction de $\mathcal{D}$ avec le système de t permutations, c'est-à-dire la suite ordonnée des $q_1 + \ldots + q_t$ requêtes et leurs réponses correspondantes (i, b, z, z'), où $i \in [1; t]$ est le numéro de la permutation, b est le bit indiquant si la requête est directe ($b = 0$) ou inverse ($b = 1$), $z \in \mathcal{I}_n$ est la requête et z' la réponse. Soit également Φ la fonction qui envoie un uplet de permutations $\boldsymbol{P} = (P_1, \ldots, P_t)$ sur la transcription de la première phase de l'attaque quand $\mathcal{D}$ interagit avec $(P_1, \ldots, P_t, *)$, où $*$ est soit une permutation UAI Q ou $\texttt{EM}_{\boldsymbol{P},k}$ (ce n'est pas important puisque $\mathcal{D}$ ne fait pas de requêtes à la permutation externe pendant la première phase de l'attaque). On dit que la transcription τ est *consistante* si il existe un uplet $\boldsymbol{P}$ tel que $\Phi(\boldsymbol{P}) = \tau$, et on note Γ l'ensemble des transcriptions consistantes. Enfin, pour une transcription consistante τ, on construit la suite $a(\tau), b(\tau) \in (\mathcal{I}_n)^{*q_1,\ldots,q_t}$: soit (i, b, z, z') la j-ème requête et réponse correspondante à P_i dans la transcription, si c'est une requête directe ($b = 0$) alors on définit $a_i^j = z$ et $b_i^j = z'$; Sinon, quand c'est une requête inverse ($b = 1$), on définit $a_i^j = z'$ et $b_i^j = z$. Notons que pour une transcription consistante τ, $\Phi(\boldsymbol{P}) = \tau$ si et seulement si $\boldsymbol{P}(a(\tau)) = b(\tau)$. Le nombre de transcriptions consistantes est égal à :

$$|\Gamma| = \prod_{i=1}^{t} (N)_{q_i} \ . \tag{3.1}$$

En effet, la première requête de $\mathcal{D}$ est fixée dans chaque exécution et on peut supposer, sans perte de généralité, que c'est une requête à P_1. Il y a exactement N réponses possibles. La requête suivante est déterminée par la réponse de la première. Si c'est à nouveau une requête à P_1 alors il y a $N - 1$ réponses possibles. Si c'est une requête à $P_i, i \neq 1$ alors il y a N réponses possibles. Et ainsi de suite. Par récurrence, on obtient facilement le résultat voulu.

L'uplet de requêtes non-adaptatives $x = (x^1, \ldots, x^{q_e}) \in (\mathcal{I}_n)^{*q_e}$ de $\mathcal{D}$ à la permutation externe est une fonction déterministe de la transcription τ de la première phase de l'attaque. Soit Ψ la fonction qui envoie une transcription consistante τ sur l'uplet de requêtes x correspondantes. La sortie de $\mathcal{D}$ est alors une fonction déterministe de τ et des réponses $y = (y^1, \ldots, y^{q_e})$ de la permutation externe ayant reçu les requêtes $\Psi(\tau)$. Pour toute transcription consistante τ, on note Σ_τ l'ensemble des y tels que $\mathcal{D}$ répond 1 quand il reçoit les réponses y aux requêtes $\Psi(\tau)$. Alors, par définition, on a :

$$\begin{aligned}
\Pr^*[\mathcal{D}(1^n) = 1] &= \sum_{\tau\in\Gamma} \sum_{y\in\Sigma_\tau} \frac{\#\{(\boldsymbol{P}, Q) \in \mathcal{P}_n^{t+1} : \Phi(\boldsymbol{P}) = \tau \wedge Q(\Psi(\tau)) = y\}}{|\mathcal{P}_n|^{t+1}} \\
&= \sum_{\tau\in\Gamma} \sum_{y\in\Sigma_\tau} \frac{\#\{(\boldsymbol{P}, Q) \in \mathcal{P}_n^{t+1} : \boldsymbol{P}(a(\tau)) = b(\tau) \wedge Q(\Psi(\tau)) = y\}}{|\mathcal{P}_n|^{t+1}} \\
&= \sum_{\tau\in\Gamma} \sum_{y\in\Sigma_\tau} \frac{1}{(N)_{q_e} \prod_{i=1}^{t} (N)_{q_i}} \ .
\end{aligned} \tag{3.2}$$

On a également :

$$\Pr\left[\mathcal{D}(1^n)=1\right] = \sum_{\tau\in\Gamma}\sum_{y\in\Sigma_\tau} \frac{\#\{(\boldsymbol{P},k)\in\Omega_t : \Phi(\boldsymbol{P})=\tau \wedge \mathtt{EM}_{\boldsymbol{P},k}(\Psi(\tau))=y\}}{|\Omega_t|} \ . \tag{3.3}$$

On utilise maintenant l'hypothèse que, pour tous $a,b\in(\mathcal{I}_n)^{*q_1,\ldots,q_t}$ et $x\in(\mathcal{I}_n)^{*q_e}$, on a $\|\mu_x(\cdot|\boldsymbol{P}(a)=b)-\mu^*_{q_e}\|\leq\alpha$. On sait également que, pour toutes distributions μ et ν sur un espace Ω, on a $\|\mu-\nu\|=\max_{S\subset\Omega}(\mu(S)-\nu(S))$. Ainsi, en utilisant le lemme 3.1 et l'hypothèse sur α, on a que pour tous les uplets a,b,x et tout sous-ensemble $S\subset(\mathcal{I}_n)^{*q_e}$:

$$\left|\sum_{y\in S}\frac{\#\{(\boldsymbol{P},k)\in\Omega_t : \boldsymbol{P}(a)=b\wedge\mathtt{EM}_{\boldsymbol{P},k}(x)=y\}}{|\Omega_t|/\prod_{i=1}^t(N)_{q_i}} - \sum_{y\in S}\frac{1}{(N)_{q_e}}\right| \leq \alpha \ .$$

Pour tout $\tau\in\Gamma$, on utilise l'inéquation précédente avec $(a,b)=(a(\tau),b(\tau))$, $x=\Psi(\tau)$, et $S=\Sigma_\tau$ pour obtenir :

$$\left|\sum_{y\in\Sigma_\tau}\frac{\#\{(\boldsymbol{P},k)\in\Omega_t : \boldsymbol{P}(a(\tau))=b(\tau)\wedge\mathtt{EM}_{\boldsymbol{P},k}(\Psi(\tau))=y\}}{|\Omega_t|} - \sum_{y\in\Sigma_\tau}\frac{1}{(N)_{q_e}\prod_{i=1}^t(N)_{q_i}}\right| \leq \frac{\alpha}{\prod_{i=1}^t(N)_{q_i}} \ . \tag{3.4}$$

En combinant les équations (3.2-3.3-3.4), et en sachant que, pour toute transcription consistante τ, on a $\Phi(\boldsymbol{P})=\tau$ si et seulement si $\boldsymbol{P}(a(\tau))=b(\tau)$, on obtient que :

$$\left|\Pr\left[\mathcal{D}(1^n)=1\right]-\Pr^*\left[\mathcal{D}(1^n)=1\right]\right| \leq \sum_{\tau\in\Gamma}\frac{\alpha}{\prod_{i=1}^t(N)_{q_i}} \ .$$

On en déduit finalement, en utilisant l'équation (3.1), que l'avantage de $\mathcal{D}$ est majoré par α. ∎

3.4.4 Diviser pour mieux régner (étape 2)

On vient de créer le lien entre l'avantage et la distance statistique (étape 1). Le problème s'écrit donc maintenant en terme de majoration de la distance statistique entre la distribution des sorties d'un schéma d'Even-Mansour itéré et la distribution uniforme, ce qui nous permettra d'utiliser le lemme 3.2 pour conclure.

Lemme 3.3. *Soient $q_1,\ldots,q_t,q_e$ des entiers positifs, $a,b\in(\mathcal{I}_n)^{*q_1,\ldots,q_t}$ et $x\in(\mathcal{I}_n)^{*q_e}$. Alors :*

$$\|\mu_x(\cdot|\boldsymbol{P}(a)=b)-\mu^*_{q_e}\| \leq 2^t\frac{q_e\prod_{i=1}^t q_i}{N^t} \ . \qquad \triangledown$$

La preuve de ce lemme est fondamentale. Elle repose sur l'utilisation du coupling et des différentes étapes de la stratégie de preuve par coupling que nous avons présentées au chapitre 2. Comme nous l'avons vu dans la section 2.2, notre stratégie, maintenant, est de « diviser pour mieux régner ». Pour comparer les deux distributions $\mu_x(\cdot|\boldsymbol{P}(a)=b)$ et $\mu^*_{q_e}$, nous allons créer une multitude de distributions intermédiaires et utiliser l'inégalité triangulaire. Nous commençons par construire ces distributions intermédiaires :

Soient $q_1, \ldots, q_t, q_e$ des entiers positifs, $a, b \in (\mathcal{I}_n)^{*q_1,\ldots,q_t}$ et $x = (x^1, \ldots, x^{q_e}) \in (\mathcal{I}_n)^{*q_e}$. Pour chaque $\ell \in [0; q_e]$, soit $(z^1, \ldots, z^{q_e})$ un uplet de requêtes telles que $z^i = x^i$ pour $i \leq \ell$ et z^i est uniformément aléatoire dans $\mathcal{I}_n \setminus \{z^1, \ldots, z^{i-1}\}$ pour $i > \ell$. Notons ν_ℓ la distribution du q_e-uplet de sorties quand $\mathtt{EM}_{\boldsymbol{P},k}$ reçoit les entrées $(z^1, \ldots, z^{q_e})$, conditionné par $\boldsymbol{P}(a) = b$. Remarquons que $\nu_0 = \mu^*_{q_e}$ puisque, pour $\ell = 0$, l'uplet d'entrées est uniformément aléatoire dans $(\mathcal{I}_n)^{*q_e}$, et $\nu_{q_e} = \mu_x(\cdot|\boldsymbol{P}(a) = b)$. Ainsi, on a :

$$\|\mu_x(\cdot|\boldsymbol{P}(a) = b) - \mu^*_{q_e}\| = \|\nu_{q_e} - \nu_0\| \leq \sum_{l=0}^{q_e-1} \|\nu_{\ell+1} - \nu_\ell\| \ . \tag{3.5}$$

Coupler les deux distributions adjacentes (étape 3)

Maintenant, comme nous l'indique l'inéquation (3.5), nous devons majorer la distance statistique entre $\nu_{\ell+1}$ et ν_ℓ, pour chaque $\ell \in [0; q_e - 1]$. Fixons $\ell \in [0; q_e - 1]$ arbitraire et construisons un coupling de $\nu_{\ell+1}$ et ν_ℓ. Si le coupling est bien construit, nous pourrons alors utiliser avantageusement le lemme du coupling 2.1 qui donne un majorant pour la distance statistique entre les deux distributions couplées. Notons que, pour $\nu_{\ell+1}$ et ν_ℓ, la $i-$ème entrée pour $i > \ell + 1$ est uniformément aléatoire. On va donc principalement s'intéresser aux $\ell + 1$ premières entrées et tronquer les suivantes qui ne rentrent pas en compte. Ainsi, $\|\nu_{\ell+1} - \nu_\ell\| = \|\nu'_{\ell+1} - \nu'_\ell\|$, où $\nu'_{\ell+1}$ et ν'_ℓ sont les distributions respectives des $\ell+1$ premières sorties du schéma. Cette propriété est assez intuitive mais la preuve est assez technique (voir [MRS09, Lemme 2]). Nous présentons cette preuve pour le schéma KAF au lemme 5.8.

Pour définir le coupling de $\nu'_{\ell+1}$ et ν'_ℓ, on considère le schéma d'Even-Mansour itéré $\mathtt{EM}_{\boldsymbol{P},k}$, où $\boldsymbol{P}$ vérifie $\boldsymbol{P}(a) = b$, qui reçoit $x' = (x^1, \ldots, x^{\ell+1})$, et donc $\mathtt{EM}_{\boldsymbol{P},k}(x')$ suit la distribution $\nu'_{\ell+1}$. Nous allons construire un second schéma d'Even-Mansour itéré $\mathtt{EM}_{\boldsymbol{P}',k'}$ qui reçoit $u = (u^1, \ldots, u^\ell, u^{\ell+1})$ et vérifie les propriétés suivantes :

1) $u^i = x^i$ pour $i = 1, \ldots, \ell$ et $u^{\ell+1}$ est uniformément aléatoire dans $\mathcal{I}_n \setminus \{x^1, \ldots, x^\ell\}$;

2) pour $i = 1, \ldots, \ell + 1$, si les sorties de la $j-$ème permutation interne dans les calculs de $\mathtt{EM}_{\boldsymbol{P},k}(x^i)$ et $\mathtt{EM}_{\boldsymbol{P}',k'}(u^i)$ sont égaux alors c'est également le cas pour toutes les permutations internes suivantes.

3) $\boldsymbol{P}'$ est uniformément aléatoire parmi les uplet de permutations vérifiant $\boldsymbol{P}'(a) = b$ et k' est uniformément aléatoire dans $(\mathcal{I}_n)^{t+1}$.

Remarquons que les propriétés 1) et 3) assurent que $\mathtt{EM}_{\boldsymbol{P}',k'}(u)$ suit bien la distribution ν'_ℓ. Notons également que $(\boldsymbol{P}', k')$ ne sera pas *indépendant* de $(\boldsymbol{P}, k)$, néanmoins, ce n'est pas nécessaire pour utiliser le lemme du coupling (au contraire, c'est la corrélation entre $(\boldsymbol{P}', k')$ et $(\boldsymbol{P}, k)$ qui permet d'utiliser de façon efficace le lemme du coupling). La seule condition nécessaire est que $\mathtt{EM}_{\boldsymbol{P},k}(x')$ et $\mathtt{EM}_{\boldsymbol{P}',k'}(u)$ suivent les bonnes distributions marginales $\nu'_{\ell+1}$ et ν'_ℓ.

On décrit maintenant de quelle façon nous construisons ce second schéma $\mathtt{EM}_{\boldsymbol{P}',k'}$. Tout d'abord, on fixe les clés égales aux clés du premier schéma, c'est-à-dire $k' = (k_0, \ldots, k_t)$. Pour construire $\boldsymbol{P}'$ (sur les points rencontrés lors du calcul de $\mathtt{EM}_{\boldsymbol{P}',k'}(u)$), on compare les calculs de $\mathtt{EM}_{\boldsymbol{P},k}(x^i)$ et $\mathtt{EM}_{\boldsymbol{P}',k'}(u^i)$ pour $i = 1, \ldots, \ell + 1$. Pour $j = 1, \ldots, t$, on définit x^i_j comme la sortie de P_j quand on calcule $\mathtt{EM}_{\boldsymbol{P},k}(x^i)$, et, de manière similaire, u^i_j comme la

sortie de P'_j quand on calcule $\mathtt{EM}_{\boldsymbol{P}',k'}(u^i)$, *i.e.*

$$x^i_j = P_j(k_{j-1} \oplus P_{j-1}(\cdots P_1(x^i \oplus k_0)\cdots))$$
$$\text{et } u^i_j = P'_j(k_{j-1} \oplus P'_{j-1}(\cdots P'_1(u^i \oplus k_0)\cdots)) \ .$$

On note également $x^i_0 = x^i$ et $u^i_0 = u^i$. Pour $j = 0, \ldots, t-1$, on utilise les règles suivantes :

i) si $u^i_j \oplus k_j \in a_{j+1}$, alors $u^i_{j+1} = P'_{j+1}(u^i_j \oplus k_j)$ est défini par la contrainte $\boldsymbol{P}'(a) = b$;

ii) si $u^i_j \oplus k_j \notin a_{j+1}$ et $x^i_j \oplus k_j \in a_{j+1}$, alors on choisit $u^i_{j+1} = P'_{j+1}(u^i_j \oplus k_j)$ uniformément aléatoire dans $\mathcal{I}_n \setminus (b_{j+1} \cup \{u^1_{j+1}, \ldots, u^{i-1}_{j+1}\})$;

iii) si $u^i_j \oplus k_j \notin a_{j+1}$ et $x^i_j \oplus k_j \notin a_{j+1}$, alors on définit $u^i_{j+1} = x^i_{j+1}$, c'est-à-dire que $P'_{j+1}(u^i_j \oplus k_j) = P_{j+1}(x^i_j \oplus k_j)$.

Remarquons que la propriété 2) est facilement déduite de ces règles et du fait que $k' = k$. Puisque $\boldsymbol{P}$ est uniformément aléatoire parmi les uplets de permutations vérifiant $\boldsymbol{P}(a) = b$, $\boldsymbol{P}'$ l'est également. En effet, ce résultat est clair pour les cas i) et ii). Pour le cas iii), $x^i_j \oplus k_j \notin a_{j+1}$ implique que x^i_{j+1} est uniformément aléatoire dans $\mathcal{I}_n \setminus (b_{j+1} \cup \{x^1_{j+1}, \ldots, x^{i-1}_{j+1}\})$, et donc u^i_{j+1} est uniformément aléatoire dans $\mathcal{I}_n \setminus (b_{j+1} \cup \{u^1_{j+1}, \ldots, u^{i-1}_{j+1}\})$. Ainsi la propriété 3) est vérifiée.

La distribution jointe de probabilité que nous venons de construire pour la variable aléatoire $(\mathtt{EM}_{\boldsymbol{P},k}(x'), \mathtt{EM}_{\boldsymbol{P}',k'}(u))$ est telle que les distributions marginales de $\mathtt{EM}_{\boldsymbol{P},k}(x')$ et $\mathtt{EM}_{\boldsymbol{P}',k'}(u)$ sont respectivement $\nu'_{\ell+1}$ et ν'_ℓ. En appliquant maintenant le lemme du coupling (lemme 2.1), on a :

$$\|\nu_{\ell+1} - \nu_\ell\| = \|\nu'_{\ell+1} - \nu'_\ell\| \leq \Pr\left[(x^1_t, \ldots, x^{\ell+1}_t) \neq (u^1_t, \ldots, u^{\ell+1}_t)\right]$$

où on a utilisé les égalitées $\mathtt{EM}_{\boldsymbol{P},k}(x^i) = x^i_t \oplus k_{t+1}$ et $\mathtt{EM}_{\boldsymbol{P}',k'}(u^i) = u^i_t \oplus k_{t+1}$. Clairement, les règles (combinées avec le fait que $u^i = x^i$ pour $i = 1, \ldots, \ell$) impliquent que $u^i_j = x^i_j$ pour $i = 1, \ldots, \ell$ et $j = 0, \ldots, t$, de telle façon que l'expression précédente se simplifie en $\|\nu_{\ell+1} - \nu_\ell\| \leq \Pr[x^{\ell+1}_t \neq u^{\ell+1}_t]$. Ainsi, il ne nous reste plus qu'à majorer la probabilité que $x^{\ell+1}_j$ et $u^{\ell+1}_j$ soient différents pour chaque valeur de j de 1 à t (dans le cas contraire, la propriété 2) impliquerait l'égalité de $x^{\ell+1}_t$ et $u^{\ell+1}_t$).

3.4.5 Majorer la probabilité de ne pas coupler (étape 4)

C'est à cette étape que le coupling montre toute son efficacité et son élégance. Nous allons voir que l'augmentation du nombre de tours n'augmente en rien la complexité de la preuve. Considérons le premier tour. A moins que $u^{\ell+1}_0 \oplus k_0 \in a_1$ ou $x^{\ell+1}_0 \oplus k_0 \in a_1$, on peut utiliser la règle iii) et obtenir que $u^{\ell+1}_1 = x^{\ell+1}_1$. Puisque a_1 est de cardinal q_1, et k_0 est uniformément aléatoire, on a que $\Pr[x^{\ell+1}_1 \neq u^{\ell+1}_1] \leq 2q_1/N$. Supposons maintenant que $x^{\ell+1}_j \neq u^{\ell+1}_j$ pour un certain $j \in [1; t-1]$. De la même manière que pour le premier tour, à moins que $u^{\ell+1}_j \oplus k_j \in a_{j+1}$ ou $x^{\ell+1}_j \oplus k_j \in a_{j+1}$, on a $u^{\ell+1}_{j+1} = x^{\ell+1}_{j+1}$, et donc $\Pr[x^{\ell+1}_{j+1} \neq u^{\ell+1}_{j+1} | x^{\ell+1}_j \neq u^{\ell+1}_j] \leq 2q_{j+1}/N$. En utilisant une chaîne de probabilités conditionnelles, on a :

$$\|\nu_{\ell+1} - \nu_\ell\| \leq \Pr[x^{\ell+1}_t \neq u^{\ell+1}_t] \leq \frac{2q_1}{N} \cdot \frac{2q_2}{N} \cdots \frac{2q_t}{N} = 2^t \frac{\prod_{i=1}^t q_i}{N^t} \ .$$

Finalement, en utilisant l'équation (3.5), on a :

$$\|\mu_x(\cdot | \boldsymbol{P}(a) = b) - \mu^*_{q_e}\| = \|\nu_{q_e} - \nu_0\| \leq 2^t \frac{q_e \prod_{i=1}^t q_i}{N^t} \ ,$$

ce qui prouve le lemme 3.3.

Remarquons que la clé k_t ne joue aucun rôle dans notre preuve et donc, un schéma d'Even-Mansour itéré sans dernière clé reste indistinguable face à un attaquant NCPA. Cette clé sera utile contre les attaques CCA. Remarquons également que notre preuve peut s'étendre facilement à un attaquant NCCA, c'est-à-dire un attaquant pouvant faire des requêtes inverses de manière non-adaptative. Néanmoins, nous omettons de présenter ce résultat qui complexifie les notations et notre objectif principal est la sécurité CCA que nous allons obtenir dans la prochaine section grâce à la sécurité NCPA.

3.4.6 Déduire un majorant de l'avantage NCPA (étape 5)

En combinant les lemmes 3.2 et 3.3, on en déduit le théorème suivant :

Théorème 3.4. *Soient $q_1, \ldots, q_t, q_e$ des entiers positifs. Alors :*

$$\mathbf{Adv}^{\mathrm{ncpa}}_{\mathcal{EM}[t]}(q_1, \ldots, q_t, q_e) \leq 2^t \frac{q_e \prod_{i=1}^{t} q_i}{N^t} \quad .$$

En particulier, pour tout entier positif q :

$$\mathbf{Adv}^{\mathrm{ncpa}}_{\mathcal{EM}[t]}(q) \leq 2^t \frac{q^{t+1}}{N^t} \quad .$$

Ce résultat reste vrai pour un schéma d'Even-Mansour itéré où l'on omet la dernière clé k_t. ♢

Concrètement, le schéma d'Even-Mansour itéré à t tours est NCPA sûr jusqu'à $\mathcal{O}(N^{\frac{t}{t+1}})$ requêtes. Cette borne est optimale (si l'on néglige les facteurs constants) au vue de l'attaque de Bogdanov *et al.* [BKL+12].

3.5 Indistinguabilité du schéma d'Even-Mansour itéré face à une attaque CCA

On s'intéresse maintenant à la sécurité du schéma d'Even-Mansour itéré face à une attaque CCA. Nous allons utiliser la technique des coefficients H et doubler le nombre de tours (étape 6 de notre stratégie de preuve par coupling) pour obtenir la sécurité CCA depuis la sécurité NCPA.

3.5.1 Sécurité CCA à l'aide de la technique des coefficients H

On considère, dans tout ce qui suit, un distingueur CCA qu'on définit comme un attaquant qui peut faire des requêtes aux permutations internes (de manière directe ou inverse) et à la permutation externe (de manière directe ou inverse) dans l'ordre qu'il veut et de manière adaptative. Ainsi, ce distingueur, contrairement au distingueur NCPA, reflète complètement la réalité d'une attaque CCA.

La technique des coefficients H, inventée par Jacques Patarin [Pat91, Pat08] en 1991, est un outil très puissant pour prouver l'indistinguabilité d'un schéma. Cette technique translate le problème cryptographique en un problème combinatoire. Ici, nous adaptons et prouvons l'un des théorèmes de cette technique au schéma d'Even-Mansour itéré et à nos notations.

Lemme 3.5. *Soient $q_1, \ldots, q_t, q_e$ des entiers positifs. Supposons qu'il existe β un réel positif tel que, pour tous $a, b \in (\mathcal{I}_n)^{*q_1,\ldots,q_t}$ et $x, y \in (\mathcal{I}_n)^{*q_e}$, on a :*

$$\Pr[\boldsymbol{P}(a) = b \wedge \mathtt{EM}_{\boldsymbol{P},k}(x) = y] \geq \frac{1-\beta}{(N)_{q_e} \prod_{i=1}^{t} (N)_{q_i}} \ .$$

Alors $\mathbf{Adv}^{\mathrm{cca}}_{\mathcal{EM}[t]}(q_1, \ldots, q_t, q_e) \leq \beta$. ▽

Démonstration. Cette preuve est très proche de celle du lemme 3.2. Fixons un $(q_1, \ldots, q_t, q_e)$-distingueur CCA $\mathcal{D}$. Soit τ la transcription de l'interaction de $\mathcal{D}$ avec le système de $t+1$ permutations, c'est-à-dire la suite ordonnée des $q_1 + \ldots + q_t + q_e$ requêtes et leurs réponses correspondantes (i, b, z, z'), où $i \in [1; t+1]$ est le numéro de la permutation, b est le bit indiquant si la requête est directe ($b = 0$) ou inverse ($b = 1$), $z \in \mathcal{I}_n$ est la requête et z' la réponse. Soit également Φ la fonction qui envoie un uplet de permutations $(\boldsymbol{P}, P_{t+1})$ à la transcription de l'attaque quand $\mathcal{D}$ interagit avec $(P_1, \ldots, P_{t+1})$. On dit que la transcription τ est *consistante* si il existe un uplet $(\boldsymbol{P}, P_{t+1})$ tel que $\Phi((\boldsymbol{P}, P_{t+1})) = \tau$, et on note Γ l'ensemble des transcriptions consistantes. Enfin, pour une transcription consistante τ, on construit la suite $a(\tau), b(\tau) \in (\mathcal{I}_n)^{*q_1,\ldots,q_t}$ et $x(\tau), y(\tau) \in (\mathcal{I}_n)^{*q_e}$: soit (i, b, z, z') la j-ème requête et réponse correspondante à P_i dans la transcription. Pour $i \leq t$, si c'est une requête directe ($b = 0$) alors on définit $a_i^j = z$ et $b_i^j = z'$ et, sinon, quand c'est une requête inverse ($b = 1$), on définit $a_i^j = z'$ et $b_i^j = z$. Pour $i = t+1$, de manière similaire, on définit $x^j = z$ et $y^j = z'$ si la requête est directe ($b = 0$), et $x^j = z'$ et $y^j = z$ si la requête est inverse ($b = 1$). Notons que pour une transcription consistante τ, $\Phi((\boldsymbol{P}, P_{t+1})) = \tau$ si et seulement si $\boldsymbol{P}(a(\tau)) = b(\tau)$ et $P_{t+1}(x(\tau)) = y(\tau)$. La sortie de $\mathcal{D}$ est une fonction déterministe de la transcription. On note Σ l'ensemble des transcriptions consistantes τ telles que $\mathcal{D}$ répond 1 quand la transcription est τ. Alors, par définition, on a :

$$\begin{aligned}
\Pr{}^{*}[\mathcal{D}(1^n) = 1] &= \sum_{\tau \in \Sigma} \frac{\#\{(\boldsymbol{P}, Q) \in (\mathcal{P}_n)^{t+1} : \Phi(\boldsymbol{P}, Q) = \tau\}}{|\mathcal{P}_n|^{t+1}} \\
&= \sum_{\tau \in \Sigma} \frac{\#\{(\boldsymbol{P}, Q) \in (\mathcal{P}_n)^{t+1} : \boldsymbol{P}(a(\tau)) = b(\tau) \wedge Q(x(\tau)) = y(\tau)\}}{|\mathcal{P}_n|^{t+1}} \\
&= \sum_{\tau \in \Sigma} \frac{1}{(N)_{q_e} \prod_{i=1}^{t} (N)_{q_i}} \ . \qquad (3.6)
\end{aligned}$$

On a également :

$$\begin{aligned}
\Pr[\mathcal{D}(1^n) = 1] &= \sum_{\tau \in \Sigma} \frac{\#\{(\boldsymbol{P}, k) \in \Omega_t : \Phi(\boldsymbol{P}, \mathtt{EM}_{\boldsymbol{P},k}) = \tau\}}{|\Omega_t|} \\
&= \sum_{\tau \in \Sigma} \Pr[\boldsymbol{P}(a(\tau) = b(\tau) \wedge \mathtt{EM}_{\boldsymbol{P},k}(x(\tau)) = y(\tau)] \ . \qquad (3.7)
\end{aligned}$$

En utilisant l'hypothèse sur β et l'équation (3.6), on a :

$$\Pr[\mathcal{D}(1^n) = 1] \geq \sum_{\tau \in \Sigma} \frac{1-\beta}{(N)_{q_e} \prod_{i=1}^{t} (N)_{q_i}} = (1-\beta) \Pr{}^{*}[\mathcal{D}(1^n) = 1] \ ,$$

et donc $\Pr^{*}[\mathcal{D}(1^n) = 1] - \Pr[\mathcal{D}(1^n) = 1] \leq \beta$. En appliquant le même raisonnement au distingueur $\mathcal{D}'$ qui sort la négation de $\mathcal{D}$, on déduit que :

$$(1 - \Pr{}^{*}[\mathcal{D}(1^n) = 1]) - (1 - \Pr[\mathcal{D}(1^n) = 1]) \leq \beta \ ,$$

et donc

$$\Pr^{*}[\mathcal{D}(1^n)=1]-\Pr[\mathcal{D}(1^n)=1]\geq-\beta\ ,$$

ce qui implique que l'avantage de $\mathcal{D}$ est majoré par β. ■

Sécurité CCA pour 1 tour

Avant de passer au cas général, on s'intéresse ici à la sécurité CCA du schéma d'Even-Mansour qui illustre assez simplement l'utilité du lemme précédent. Ce résultat est en fait un cas particulier du théorème 3.1 de [KR01] où $\kappa=0$.

Théorème 3.6. *Soient q_1, q_e des entiers positifs. Alors :*

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathcal{EM}[1]}(q_1,q_e)\leq\frac{2q_1q_e}{N}\ . \qquad \diamondsuit$$

Pour prouver ce thèorème, on applique le lemme 3.5 au résultat suivant :

Lemme 3.7. *Pour tous $a_1,b_1\in(\mathcal{I}_n)^{*q_1}$ et $x,y\in(\mathcal{I}_n)^{*q_e}$, on a :*

$$\Pr\left[P_1(a_1)=b_1\wedge\mathtt{EM}_{P_1,(k_0,k_1)}(x)=y\right]\geq\frac{1-2q_1q_e/N}{(N)_{q_1}(N)_{q_e}}\ . \qquad \triangledown$$

Démonstration. Fixons $a_1=(a_1^1,\ldots,a_1^{q_1})$, $b_1=(b_1^1,\ldots,b_1^{q_1})$, $x=(x^1,\ldots,x^{q_e})$ et $y=(y^1,\ldots,y^{q_e})$. Suivant les notations de [EM97], on introduit la définition suivante :

Définition 3.3
On dit qu'une paire de clés (k_0,k_1) est bonne si

$$\begin{cases} k_0\notin\{x^i\oplus a_1^j, i\in[1;q_e], j\in[1;q_1]\}\\ k_1\notin\{y^i\oplus b_1^j, i\in[1;q_e], j\in[1;q_1]\}\end{cases}$$

et mauvaise sinon. ⧫

Il y a au plus q_eq_1 mauvaises valeurs pour k_0, ainsi que pour k_1, et donc le nombre de paires de clés bonnes est au moins :

$$(N-q_eq_1)(N-q_eq_1)\geq(N^2-2Nq_1q_e)\ .$$

Fixons une bonne paire de clés (k_0,k_1). On compte maintenant le nombre de permutations P_1 telles que $P_1(a_1)=b_1$ et $\mathtt{EM}_{P_1,(k_0,k_1)}(x)=y$. Les équations $P_1(a_1)=b_1$ imposent q_1 contraintes sur P_1. Puisque la paire (k_0,k_1) est bonne, les équations $\mathtt{EM}_{P_1,(k_0,k_1)}(x)=y$ imposent q_e contraintes additionnelles (et distinctes) sur P_1. Ainsi, le nombre de permutations est exactement $N!/(N)_{q_1+q_e}$. En sommant sur toutes les paires de clés bonnes, on a que :

$$\begin{aligned}\Pr\left[P_1(a_1)=b_1\wedge\mathtt{EM}_{P_1,(k_0,k_1)}(x)=y\right]&=\frac{\#\{(P_1,k_0,k_1):P_1(a_1)=b_1\wedge\mathtt{EM}_{P_1,(k_0,k_1)}(x)=y\}}{N^2\cdot N!}\\&\geq\frac{(N^2-2Nq_1q_e)N!/(N)_{q_1+q_e}}{N^2\cdot N!}\\&\geq\frac{1-2q_1q_e/N}{(N)_{q_1}(N)_{q_e}}\ ,\end{aligned}$$

où on a utilisé le fait que $(N)_{q_1+q_e}\leq(N)_{q_1}(N)_{q_e}$. Cela prouve le lemme. ■

3.5.2 Doubler les tours pour majorer l'avantage CCA (étape 6)

Avant de présenter le lemme important de cette sous-section, nous avons besoin du lemme technique suivant :

Lemme 3.8. *Soient Ω un ensemble fini et ν la distribution uniforme sur Ω. Soit μ la distribution de probabilité sur Ω telle que $\|\mu - \nu\| \leq \varepsilon$. Alors, il existe un ensemble $S \subset \Omega$ tel que :*
- $|S| \geq (1 - \sqrt{\varepsilon})|\Omega|$
- $\forall x \in S$, $\mu(x) \geq (1 - \sqrt{\varepsilon})\nu(x)$ ▽

Démonstration. Définissons S par $S = \{x \in \Omega : \mu(x) \geq (1 - \sqrt{\varepsilon})\nu(x)\}$. On va montrer que $|S| \geq (1 - \sqrt{\varepsilon})|\Omega|$. Par l'absurde, supposons que $|S| < (1 - \sqrt{\varepsilon})|\Omega|$, ou de manière équivalente $|\bar{S}| > \sqrt{\varepsilon}|\Omega|$, *i.e.* $\nu(\bar{S}) > \sqrt{\varepsilon}$. Par définition, pour tout $x \in \bar{S}$, $\nu(x) - \mu(x) > \sqrt{\varepsilon}\nu(x)$. Ainsi :

$$\nu(\bar{S}) - \mu(\bar{S}) > \sqrt{\varepsilon}\nu(\bar{S}) > (\sqrt{\varepsilon})^2 = \varepsilon \ ,$$

en contradiction avec $\|\mu - \nu\| \leq \varepsilon$. ■

Dans le lemme suivant, nous allons composer deux schémas d'Even-Mansour (qu'on sait NCPA sûrs) pour obtenir un schéma d'Even-Mansour qu'on prouvera, par la suite, CCA sûr à l'aide du lemme 3.5.

Lemme 3.9. *Soient $t \geq 2$ un entier pair et $t' = t/2$. Soient $q_1, \ldots, q_t, q_e$ des entiers positifs. On note :*

$$\alpha_1 = 2^{t'} \frac{q_e \prod_{i=1}^{t'} q_i}{N^{t'}} \quad et \quad \alpha_2 = 2^{t'} \frac{q_e \prod_{i=t'+1}^{t} q_i}{N^{t'}} \ .$$

Alors, pour tous les uplets $a, b \in (\mathcal{I}_n)^{*q_1,\ldots,q_t}$ et $x, y \in (\mathcal{I}_n)^{*q_e}$, on a :

$$\Pr[\boldsymbol{P}(a) = b \wedge \mathtt{EM}_{\boldsymbol{P},k}(x) = y] \geq \frac{1 - \beta}{(N)_{q_e} \prod_{i=1}^{t} (N)_{q_i}} \ ,$$

où $\beta = 2(\sqrt{\alpha_1} + \sqrt{\alpha_2})$. ▽

Démonstration. Tout d'abord, on modifie légèrement la façon dont le schéma d'Even-Mansour itéré à $2t'$ tours est construit afin de l'écrire comme la composition de deux schémas d'Even-Mansour itérés à t' tours. Pour cela, on écrit la clé du milieu $k_{t'}$ entre $P_{t'}$ et $P_{t'+1}$ comme le xor de deux clés indépendantes $k^1_{t'}$ et $k^2_{t'}$, et on redéfinit $\mathtt{EM}_{\boldsymbol{P},k}$ où $\boldsymbol{P} = (P_1, \ldots, P_{2t'}) \in (\mathcal{P}_n)^{2t'}$ et $k = (k_0, \ldots, k_{t'-1}, k^1_{t'}, k^2_{t'}, k_{t'+1}, \ldots, k_{2t'}) \in (\mathcal{I}_n)^{2t'+2}$, par :

$$\mathtt{EM}_{\boldsymbol{P},k} = \underbrace{\oplus_{k_{2t'}} \circ P_{2t'} \circ \oplus_{k_{2t'-1}} \circ \cdots \circ P_{t'+1} \circ \oplus_{k^2_{t'}}}_{\mathtt{EM}_{\boldsymbol{P}_2,\tilde{k}_2}} \circ \underbrace{\oplus_{k^1_{t'}} \circ P_{t'} \circ \cdots \circ \oplus_{k_1} \circ P_1 \circ \oplus_{k_0}}_{\mathtt{EM}_{\boldsymbol{P}_1,\tilde{k}_1}} \ .$$

Clairement, cela ne modifie pas la probabilité $\Pr[\boldsymbol{P}(a) = b \wedge \mathtt{EM}_{\boldsymbol{P},k}(x) = y]$ puisque $k^1_{t'} \oplus k^2_{t'}$ est uniformément aléatoire quand $k^1_{t'}$ et $k^2_{t'}$ le sont. Cela permet d'écrire $\mathtt{EM}_{\boldsymbol{P},k} =$

$\mathtt{EM}_{\boldsymbol{P}_2,\tilde{k}_2} \circ \mathtt{EM}_{\boldsymbol{P}_1,\tilde{k}_1}$, où $\boldsymbol{P}_1 = (P_1, \ldots, P_{t'})$, $\boldsymbol{P}_2 = (P_{t'+1}, \ldots, P_{2t'})$, $\tilde{k}_1 = (k_0, \ldots, k_{t'-1}, k^1_{t'})$, $\tilde{k}_2 = (k^2_{t'}, k_{t'+1}, \ldots, k_{2t'})$. On note maintenant $\widetilde{\Omega}_{2t'} = (\mathcal{P}_n)^{2t'} \times (\mathcal{I}_n)^{2t'+2}$. Ainsi $|\widetilde{\Omega}_{2t'}| = |\Omega_{t'}|^2$.

Fixons $a, b \in (\mathcal{I}_n)^{*q_1,\ldots,q_t}$ et $x, y \in (\mathcal{I}_n)^{*q_e}$. On note $\tilde{a}_1 = (a_1, \ldots, a_{t'})$, $\tilde{a}_2 = (a_{t'+1}, \ldots, a_{2t'})$, $\tilde{b}_1 = (b_1, \ldots, b_{t'})$, et $\tilde{b}_2 = (b_{t'+1}, \ldots, b_{2t'})$. Appliquons le lemme 3.8 indépendamment aux deux moitiés du schéma $\mathtt{EM}_{\boldsymbol{P}_1,\tilde{k}_1}$ et $\mathtt{EM}_{\boldsymbol{P}_2,\tilde{k}_2}$. Le lemme 3.3 implique que $\|\mu^1_x(\cdot|\boldsymbol{P}_1(\tilde{a}_1) = \tilde{b}_1) - \mu^*_{q_e}\| \leq \alpha_1$, où $\mu^1_x(\cdot|\boldsymbol{P}_1(\tilde{a}_1) = \tilde{b}_1)$ est la distribution de $\mathtt{EM}_{\boldsymbol{P}_1,\tilde{k}_1}(x)$ conditionnée sur $\boldsymbol{P}_1(\tilde{a}_1) = \tilde{b}_1$. Ainsi, le lemme 3.8 assure l'existence d'un sous-ensemble $S_x \subset (\mathcal{I}_n)^{*q_e}$ de taille au moins $(1 - \sqrt{\alpha_1})(N)_{q_e}$ tel que, pour tout $z \in S_x$:

$$\begin{aligned}\mu^1_x(z|\boldsymbol{P}_1(\tilde{a}_1) = \tilde{b}_1) &= \frac{\#\{(\boldsymbol{P}_1, \tilde{k}_1) \in \Omega_{t'} : \boldsymbol{P}_1(\tilde{a}_1) = \tilde{b}_1 \wedge \mathtt{EM}_{\boldsymbol{P}_1,\tilde{k}_1}(x) = z\}}{|\Omega_{t'}| / \prod_{i=1}^{t'}(N)_{q_i}} \\ &\geq (1 - \sqrt{\alpha_1})\frac{1}{(N)_{q_e}} \ .\end{aligned}$$

De même, en appliquant le même raisonnement à la distribution $\mu^2_y(\cdot|\boldsymbol{P}_2(\tilde{a}_2) = \tilde{b}_2)$ de $\mathtt{EM}^{-1}_{\boldsymbol{P}_2,\tilde{k}_2}(y)$ conditionnée par $\boldsymbol{P}_2(\tilde{a}_2) = \tilde{b}_2$, on obtient l'existence d'un sous-ensemble $S_y \subset (\mathcal{I}_n)^{*q_e}$ de taille au moins $(1 - \sqrt{\alpha_2})(N)_{q_e}$ tel que, pour tout $z \in S_y$:

$$\begin{aligned}\mu^2_y(z|\boldsymbol{P}_2(\tilde{a}_2) = \tilde{b}_2) &= \frac{\#\{(\boldsymbol{P}_2, \tilde{k}_2) \in \Omega_{t'} : \boldsymbol{P}_2(\tilde{a}_2) = \tilde{b}_2 \wedge \mathtt{EM}^{-1}_{\boldsymbol{P}_2,\tilde{k}_2}(y) = z\}}{|\Omega_{t'}| / \prod_{i=t'+1}^{t}(N)_{q_i}} \\ &\geq (1 - \sqrt{\alpha_2})\frac{1}{(N)_{q_e}} \ .\end{aligned}$$

On peut maintenant minorer le nombre de $(\boldsymbol{P}, k) \in \widetilde{\Omega}_{2t'}$ vérifiant $\boldsymbol{P}(a) = b$ et $\mathtt{EM}_{\boldsymbol{P},k}(x) = y$ en sommant, sur les valeurs intermédiaires $z \in S_x \cap S_y$, le produit du nombre de $(\boldsymbol{P}_1, \tilde{k}_1) \in \Omega_{t'}$ vérifiant $\boldsymbol{P}_1(\tilde{a}_1) = \tilde{b}_1$ et $\mathtt{EM}_{\boldsymbol{P}_1,\tilde{k}_1}(x) = z$ et le nombre de $(\boldsymbol{P}_2, \tilde{k}_2) \in \Omega_{t'}$ vérifiant $\boldsymbol{P}_2(\tilde{a}_2) = \tilde{b}_2$ et $\mathtt{EM}_{\boldsymbol{P}_2,\tilde{k}_2}(z) = y$. En combinant les deux équations précédentes, on a :

$$\#\{(\boldsymbol{P}, k) \in \widetilde{\Omega}_{2t'} : \boldsymbol{P}(a) = b \wedge \mathtt{EM}_{\boldsymbol{P},k}(x) = y\} \geq \frac{|S_x \cap S_y|(1 - \sqrt{\alpha_1})(1 - \sqrt{\alpha_2})|\Omega_{t'}|^2}{((N)_{q_e})^2 \prod_{i=1}^{t}(N)_{q_i}} \ .$$

Finalement, en notant que $|S_x \cap S_y| \geq (1 - \sqrt{\alpha_1} - \sqrt{\alpha_2})(N)_{q_e}$, en divisant chaque terme par $|\Omega_{t'}|^2 = |\widetilde{\Omega}_{2t'}|$, et en utilisant :

$$(1 - \sqrt{\alpha_1} - \sqrt{\alpha_2})(1 - \sqrt{\alpha_1})(1 - \sqrt{\alpha_2}) \geq 1 - 2(\sqrt{\alpha_1} + \sqrt{\alpha_2}) \ ,$$

on obtient que :

$$\Pr[\boldsymbol{P}(a) = b \wedge \mathtt{EM}_{\boldsymbol{P},k}(x) = y] \geq \frac{1 - \beta}{(N)_{q_e} \prod_{i=1}^{t}(N)_{q_i}} \ ,$$

avec $\beta = 2(\sqrt{\alpha_1} + \sqrt{\alpha_2})$, ce qui termine la preuve. ∎

En combinant les lemmes 3.5 et 3.9, on obtient finalement notre théorème principal :

Théorème 3.10. *Soient $t \geq 2$ un entier pair et $t' = t/2$. Soient $q_1, \ldots, q_t, q_e$ des entiers positifs. Alors :*

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathcal{EM}[t]}(q_1, \ldots, q_t, q_e) \leq \left(\frac{2^{t'+2} q_e \prod_{i=1}^{t'} q_i}{N^{t'}}\right)^{1/2} + \left(\frac{2^{t'+2} q_e \prod_{i=t'+1}^{t} q_i}{N^{t'}}\right)^{1/2} .$$

En particulier, pour tout entier positif q :

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathcal{EM}[t]}(q) \leq 2^{t/4+3} \frac{q^{(t+2)/4}}{N^{t/4}} .$$

Pour t impair, on a $\mathbf{Adv}^{\mathrm{cca}}_{\mathcal{EM}[t]} \leq \mathbf{Adv}^{\mathrm{cca}}_{\mathcal{EM}[t-1]}$, et on peut donc utiliser la borne ci-dessus avec $t-1$. ♢

Concrètement, nous avons prouvé que le schéma d'Even-Mansour itéré à t tours est CCA sûr jusqu'à $\mathcal{O}(N^{\frac{t}{t+2}})$ requêtes.

Chapitre 4

Preuve d'indistinguabilité du schéma de chiffrement par blocs CLRW

4.1 Les schémas de chiffrement par blocs paramétrables

Définitions et motivations

Pour deux ensembles $\mathcal{D}$ et $\mathcal{K}$, on note $\mathsf{BC}(\mathcal{K}, \mathcal{D})$ l'ensemble des schémas de chiffrement par blocs ayant pour domaine $\mathcal{D}$ et espace des clés $\mathcal{K}$, c'est-à-dire l'ensemble des fonctions $E : \mathcal{K} \times \mathcal{D} \to \mathcal{D}$ telles que, pour tout $k \in \mathcal{K}, E(k, \cdot) \in \mathrm{Perm}(\mathcal{D})$. Introduits par Liskov, Rivest, et Wagner [LRW02], les schémas de chiffrement par blocs paramétrables (TBC pour « Tweakable BlockCiphers ») sont des schémas de chiffrement admettant un paramètre publique supplémentaire dit « tweak », c'est-à-dire des schémas de chiffrement par blocs indexés par un paramètre public t, le tweak. Plus précisément, pour trois ensembles $\mathcal{D}, \mathcal{K}$ et $\mathcal{T}$, on note $\mathsf{TBC}(\mathcal{K}, \mathcal{T}, \mathcal{D})$ l'ensemble des schémas de chiffrement par blocs paramétrables, c'est-à-dire l'ensemble des fonctions $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{D} \to \mathcal{D}$ telles que, pour tout tweak $t \in \mathcal{T}$, $\widetilde{E}(\cdot, t, \cdot) \in \mathsf{BC}(\mathcal{K}, \mathcal{D})$.

A quoi sert un schéma de chiffrement par blocs paramétrable ? On s'est rendu compte que de nombreux modes d'opérations et d'autres applications utilisant des schémas de chiffrement par blocs ont besoin d'instances différentes du schéma utilisé afin d'éviter des attaques comme, par exemple, permuter certains blocs en entrée. Pour pallier à ce problème, on peut utiliser des clés différentes et utiliser une instance du schéma par clé mais on perd en efficacité. On peut également modifier l'entrée ou la sortie avant ou après avoir appliqué le schéma. Ces techniques tentent de résoudre un problème provenant d'un manque de variabilité du schéma de chiffrement. En ajoutant un paramètre supplémentaire, le tweak, on résout ce problème à la racine, c'est-à-dire en modifiant le schéma de chiffrement. En pratique, changer le tweak est beaucoup moins coûteux que changer la clé, ce qui permet de faire varier la fonction de chiffrement à un coût faible. C'est très pratique pour le chiffrement d'un disque dur ou d'une base de donnée par exemple. Ce nouveau paramètre permet d'apporter de la variabilité au schéma. Le tweak étant public, il est donc connu de l'attaquant et on considère donc un modèle d'attaquant qui peut choisir le tweak correspondant à sa requête. Il n'a, bien sûr, pas accès à la clé.

Quelques constructions de TBCs

Il n'y a que très peu de constructions de schémas de chiffrement par blocs qui sont paramétrables « par construction ». On peut noter le schéma de chiffrement Hasty Pudding [Sch98], Mercy [Cro00], et Threefish, le schéma de chiffrement par blocs utilisé pour la fonction hash Skein [FLS+10]. Goldenberg *et al.* [GHL+07] ont également considéré la possibilité d'incorporer un tweak dans une structure de Feistel. La plupart du temps, les constructions proposées partent d'un schéma de chiffrement par blocs et incorporent un tweak au schéma.

Une propriété importante d'un TBC est l'efficacité d'une modification du tweak car, la plupart du temps, changer la clé dans un schéma de chiffrement par blocs est une opération coûteuse et le tweak sera très utile si il est bien plus profitable de changer le tweak que la clé. Ainsi, on évite de construire des TBCs qui nécessitent un changement de clé si il y a un changement de tweak. Qu'en est-il de la sécurité de ces schémas ?

Les constructions de schémas de chiffrement par blocs paramétrables proposées par Liskov *et al.* [LRW02], ou les constructions XE et XEX de Rogaway [Rog04], sont prouvées sûres jusqu'à la borne des anniversaires, c'est-à-dire jusqu'à $\mathcal{O}(N^{1/2})$ requêtes au schéma, où n est le nombre de bits par blocs et $N = 2^n$ la taille du domaine. La première construction d'un TBC qui dépasse la borne des anniversaires est due à Minematsu [Min09]. Néanmoins, cette construction est restrictive sur la longueur du tweak et, surtout, impose de modifier la clé lorsque l'on modifie le tweak. Il faut attendre 2012 et les travaux de Landecker, Shrimpton, et Terashima [LST12] pour obtenir une construction d'un TBC qui ne nécessite pas de modifier la clé pour changer le tweak et qui permet de dépasser la borne des anniversaires. Leur construction repose sur une construction plus ancienne, appelée LRW2 (voir figure 4.1), proposée par [LRW02] et définie par : étant donné un schéma de chiffrement E avec espace des clés $\mathcal{K}$ et une famille $\mathcal{H}$ de fonctions ε-AXU$_2$ (c'est-à-dire que tous x, x', y vérifie $\Pr[h \leftarrow_{\$} \mathcal{H} : h(x) \oplus h(x') = y] \leq \varepsilon$), on définit le schéma de chiffrement $\widetilde{E}$ ayant pour espace des clés $\mathcal{K} \times \mathcal{H}$ et vérifiant, $\forall (k,h) \in \mathcal{K} \times \mathcal{H}, \forall (t,x) \in \mathcal{T} \times \mathcal{I}_n$:

$$\widetilde{E}_{k,h}(t,x) := h(t) \oplus E_k(x \oplus h(t)) \ .$$

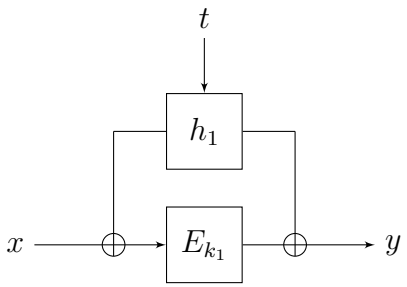

FIGURE 4.1 – Le schéma de chiffrement par blocs paramétrable LRW2.

Cette construction est prouvée sûre jusqu'à la borne des anniversaires ($\mathcal{O}(N^{1/2})$ requêtes) face à une attaque CCA et pour un schéma E indistinguable d'une permutation aléatoire face à une attaque CCA pour ce nombre de requêtes. Elle a également l'avantage de ne pas restreindre le format du tweak, il suffit d'ajuster la famille $\mathcal{H}$.

En 2012, Landecker, Shrimpton, et Terashima [LST12] proposent d'étendre le schéma LRW2 de [LRW02] à 2 tours. Ils définissent ce schéma « Chained LRW2 » ou CLRW2

(voir figure 4.2) tel que, $\forall(k_1,k_2,h_1,h_2) \in \mathcal{K}^2 \times \mathcal{H}^2, \forall(t,x) \in \mathcal{T} \times \mathcal{I}_n$:

$$\widetilde{E}_{(k_1,k_2),(h_1,h_2)}(t,x) = h_2(t) \oplus E_{k_2}\Big(h_1(t) \oplus E_{k_1}\big(x \oplus h_1(t)\big) \oplus h_2(t)\Big) \ .$$

Ils prouvent que ce schéma est sûr jusqu'à $\mathcal{O}(N^{2/3})$ requêtes d'un attaquant CCA.

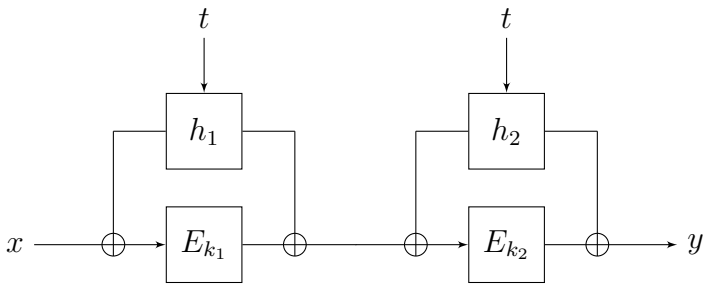

FIGURE 4.2 – Le schéma de chiffrement par blocs paramétrable $\texttt{CLRW}^{2,E,\mathcal{H}}$.

Contribution

En étudiant les travaux de [LST12] sur le schéma CLRW2, on peut naturellement se demander de quelle manière la borne de sécurité évolue si on ajoute encore des tours au schéma. Cette étude est l'objet de notre article présenté à FSE 2013 [LS13b], en collaboration avec Yannick SEURIN, où nous remarquons que, comme pour le schéma d'Even-Mansour itéré, le schéma peut être généralisé à plusieurs tours et que la borne de sécurité s'améliore. Nous appelons simplement cette construction étendue le schéma CLRW à r tours (ou r-CLRW). Nous avons ici étudié la sécurité de ce schéma pour un nombre arbitraire de tours en utilisant la technique du coupling. Là encore, nous avons obtenu un résultat optimal pour une sécurité NCPA (jusqu'à $\mathcal{O}(N^{\frac{r}{r+1}})$ requêtes pour r tours) et une sécurité asymptotiquement optimale pour la sécurité CCA (jusqu'à $\mathcal{O}(N^{\frac{r}{r+2}})$ requêtes pour r tours avec r pair. Pour obtenir la sécurité CCA, nous avons prouvé un théorème général sur la composition de TBCs qui, étant donné deux TBCs $\widetilde{E}$ et $\widetilde{E'}$ NCPA sûrs, prouve que la composition $\widetilde{E'}^{-1} \circ \widetilde{E}$ est un TBC sûr face aux attaques CCA. Ce théorème généralise donc aux TBCs un résultat que nous avons utilisé pour le schéma d'Even-Mansour itéré qui consiste à composer deux schémas NCPA sûr pour obtenir un schéma CCA sûrs.

La première partie de notre preuve consiste à prouver la sécurité NCPA d'un r-CLRW. Cette preuve présente à la fois de grandes similitudes et de grandes différences avec ce que nous avons fait pour le schéma d'Even-Mansour itéré (voir section 3.4). Dans les deux cas, nous avons utilisé la technique du coupling en appliquant la même stratégie de déplacer le problème cryptographique, calcul de l'avantage, à un calcul probabiliste, calcul de la distance statistique, (étape 1) puis nous avons « divisé pour mieux régner » en considérant une multitude de distributions intermédiaires et en ramenant le problème initial au calcul de la distance statistique entre deux distributions adjacentes (étape 2). L'étape suivante consiste à coupler les distributions adjacentes. Ici, il y a une très grande différence entre les deux schémas. Dans le schéma d'Even-Mansour itéré, les permutations internes $P_1, \ldots, P_t$ sont publiques et accessibles à l'attaquant, tandis que, dans le schéma r-CLRW, les permutations $E_{k_1}, \ldots, E_{k_r}$ sont « cachées ». Dans le schéma d'Even-Mansour

itéré, les clés sont tirées au début et restent fixes pour la suite de l'attaque, tandis que, dans le schéma r-CLRW, les valeurs $h_i(t)$ (qui peuvent être vues comme l'analogue des clés pour le schéma d'Even-Mansour itéré) peuvent être « rafraîchies » par l'attaquant en modifiant le tweak t. Dans les deux cas, la preuve de sécurité repose sur une majoration de la probabilité que l'attaquant déclenche une chaîne de collisions en entrée des permutations internes (mais la façon dont l'attaquant déclenche de telles collisions est assez différente d'un schéma à l'autre).

Application au TBC-MAC

Comme application de la primitive TBC, [LRW02] ont proposé la construction TBC-MAC : étant donné $k, n > 0$, $\widetilde{E} : \{0,1\}^k \times \mathcal{I}_n \times \mathcal{I}_n \to \mathcal{I}_n$ un TBC, $t_0 \in \mathcal{I}_n$ fixé, alors, pour toute clé $k \in \{0,1\}^k$ et tout message $m = m_1, \ldots, m_b$ constitué de blocs de n-bits, on a

$$\text{TBCMAC}[\widetilde{E}]_k(m) = t_b \text{ où } t_i \leftarrow \widetilde{E}(t_{i-1}, k, m_i) \text{ pour tout } i \in [1; b] \ .$$

On remarque que la construction TBC-MAC est analogue au CBC-MAC puisque, si $\widetilde{E}(t, k, x) = E(t \oplus x, k)$, on obtient la construction CBC-MAC. Dans [LST12], les auteurs prouvent que TBC-MAC a, comme le CBC-MAC, une sécurité jusqu'à la borne des anniversaires. Ils proposent alors une nouvelle construction TBCMAC2, autorisant des tweaks de longueurs plus variables et plus grandes, et aussi sûre que la primitive TBC utilisée. Étant donnés $k, n, b > 0$, un TBC $\widetilde{E} : \{0,1\}^k \times \{0,1\}^{n+b+1} \times \{0,1\}^n \to \mathcal{I}_n$, un message de $\ell > 1$ blocs $m_1, \ldots, m_\ell$, un « nonce » $n \in \{0,1\}^b$ (un nonce est un nombre arbitraire dont on ne se sert, en théorie, qu'une fois), et une valeur initiale fixée $t_0 = IV$, on définit TBCMAC2$[\widetilde{E}]$ par

$$\text{TBCMAC2}[\widetilde{E}]_k(n, m) = t_\ell = \widetilde{E}_k(t_{\ell-1}||1||n, m_\ell),$$

où, pour $i = 1$ à $\ell - 1$, $t_i = \widetilde{E}_k(t_{i-1}||0||0^b, m_i)$. On dit qu'un attaquant est « nonce-respecting » si il ne répète jamais un nonce. Alors, cette construction est aussi sûre que la primitive $\widetilde{E}$ utilisée face à un attaquant nonce-respecting (Théorème 3 de [LST12]).

Ainsi, en instanciant avec un $\texttt{CLRW}^{2,E,\mathcal{H}}$, ils obtiennent un MAC avec une sécurité jusqu'à $\mathcal{O}(N^{2/3})$ requêtes. En appliquant le même raisonnement, en instanciant avec un r-CRLW, nous obtenons un MAC avec une sécurité jusqu'à $\mathcal{O}(N^{r/(r+2)})$ requêtes, pour r pair. Les schémas MAC ayant une sécurité dépassant la borne des anniversaires sont assez rares. On peut citer Yasuda [Yas10, Yas11] et Dodis et Steinberger [DS11].

Problèmes ouverts

Nous conjecturons que la construction r-CLRW est sûre jusqu'à $\mathcal{O}(N^{r/(r+1)})$ requêtes et non $\mathcal{O}(N^{r/(r+2)})$ requêtes comme nous le prouvons, contre une attaque CCA. Cet écart entre notre preuve et la borne optimale est similaire à celui que nous avons avec le schéma d'Even-Mansour itéré. Il est légitime de penser que la preuve de Chen et Steinberger [CS14] puisse s'ajuster au schéma r-CLRW pour prouver une borne optimale, de la même manière qu'ils l'ont fait pour le schéma d'Even-Mansour itéré. Malgré nos efforts, nous ne sommes pas encore parvenus à résoudre ce problème. L'écart entre la borne prouvée et la borne optimale est asymptotiquement nul mais important pour les premières valeurs de r. Par exemple, nous prouvons une sécurité CCA jusqu'à $\mathcal{O}(N^{3/4})$ requêtes pour 6 tours mais nous conjecturons que c'est déjà le cas pour 3 tours. Nous conjecturons que notre preuve

utilise deux fois plus de tours que nécessaire. Cela provient de notre théorème qui consiste à doubler les tours pour obtenir la sécurité CCA en fonction de la sécurité NCPA (obtenue par coupling).

Il est également intéressant d'étudier comment diminuer le nombre de clés pour obtenir un schéma plus pratique qui reste sûr.

4.2 La construction r-CLRW

Dans cette section, nous présentons notre construction r-CLRW.

4.2.1 Notations et définitions

Nous introduisons ici des définitions et des notations liées à la construction r-CLRW et à l'étude de sa sécurité.

Schéma de chiffrement par blocs parfait

Pour un TBC $\widetilde{E}$, on note $\widetilde{E}_k(\cdot,\cdot)$ la fonction $\widetilde{E}(k,\cdot,\cdot)$. On note $\mathsf{BC}(\mathcal{K},n)$ (resp. $\mathsf{TBC}(\mathcal{K},\mathcal{T},n)$) l'ensemble des schémas de chiffrement par blocs (resp. TBC) ayant pour domaine $\mathcal{D} = \{0,1\}^n$. Le *schéma de chiffrement par blocs parfait* sur $\mathcal{D}$ est défini comme le schéma de chiffrement par blocs ayant pour espace des clés $\mathrm{Perm}(\mathcal{D})$. Quand le domaine est clairement connu ($\mathcal{D} = \{0,1\}^n$ la plupart du temps), on notera E^* le schéma de chiffrement par blocs parfait sur $\mathcal{D}$. Tirer une clé pour E^* correspond à tirer une permutation aléatoirement dans $\mathrm{Perm}(\mathcal{D})$.

Soit q un entier $q \leq |\mathcal{D}|$. Etant donné un uplet $t = (t_1,\ldots,t_q) \in \mathcal{T}^q$, on note $\Omega_t \subset \mathcal{D}^q$ l'ensemble des entrées possibles $x = (x_1,\ldots,x_q) \in \mathcal{D}^q$ telles que toutes les paires (t_i,x_i) sont deux à deux distinctes :

$$\Omega_t = \{x := (x_1,\ldots,x_q) \in \mathcal{D}^q : (x_i,t_i) \neq (x_j,t_j), \forall i \neq j\} \quad .$$

Définition des avantages

Soient $\mathcal{D},\mathcal{K},\mathcal{T}$ des ensembles, $E \in \mathsf{BC}(\mathcal{K},\mathcal{D})$ un schéma de chiffrement par blocs et $\widetilde{E} \in \mathsf{TBC}(\mathcal{K},\mathcal{T},\mathcal{D})$ un TBC. Un attaquant $\mathcal{A}$ est dit non-adaptatif si toutes les requêtes sont choisies à l'avance (avant de faire des requêtes à l'oracle), et adaptatif sinon. Pour tous q,τ, on définit les avantages suivants (où, suivant l'espace de probabilité, on a $k \leftarrow_{\$} \mathcal{K}$, $\pi \leftarrow_{\$} \mathrm{Perm}(\mathcal{D})$, ou $\widetilde{\pi} \leftarrow_{\$} \mathsf{BC}(\mathcal{T},\mathcal{D})$) :

$$\begin{aligned}
\mathbf{Adv}^{\mathrm{ncpa}}_{E}(q,\tau) &= \max_{\mathcal{A}} \left|\Pr\left[\mathcal{A}^{E_k(\cdot)} \Rightarrow 1\right] - \Pr\left[\mathcal{A}^{\pi(\cdot)} \Rightarrow 1\right]\right| \\
\mathbf{Adv}^{\mathrm{cca}}_{E}(q,\tau) &= \max_{\mathcal{A}} \left|\Pr\left[\mathcal{A}^{E_k(\cdot),E_k^{-1}(\cdot)} \Rightarrow 1\right] - \Pr\left[\mathcal{A}^{\pi(\cdot),\pi^{-1}(\cdot)} \Rightarrow 1\right]\right| \\
\mathbf{Adv}^{\widetilde{\mathrm{ncpa}}}_{\widetilde{E}}(q,\tau) &= \max_{\mathcal{A}} \left|\Pr\left[\mathcal{A}^{\widetilde{E}_k(\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\mathcal{A}^{\widetilde{\pi}(\cdot,\cdot)} \Rightarrow 1\right]\right| \\
\mathbf{Adv}^{\widetilde{\mathrm{cca}}}_{\widetilde{E}}(q,\tau) &= \max_{\mathcal{A}} \left|\Pr\left[\mathcal{A}^{\widetilde{E}_k(\cdot,\cdot),\widetilde{E}_k^{-1}(\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\mathcal{A}^{\widetilde{\pi}(\cdot,\cdot),\widetilde{\pi}^{-1}(\cdot,\cdot)} \Rightarrow 1\right]\right| \quad ,
\end{aligned}$$

où, pour ncpa et $\widetilde{\mathrm{ncpa}}$ (resp. cca et $\widetilde{\mathrm{cca}}$), le max est pris sur tous les attaquants non-adaptatifs (resp. adaptatifs) faisant au plus q requêtes à l'oracle et agissant en temps au

plus τ. Les probabilités sont calculées sur l'aléa utilisé par l'attaquant et sur les tirages aléatoires de k, π ou $\widetilde{\pi}$ suivant les cas. On note $\widetilde{\pi}$ la *permutation paramétrable* (bien que cet objet soit syntaxiquement similaire à un schéma de chiffrement par blocs) qui prend un tweak en première entrée plutôt qu'une clé.

Définition 4.1
Soit S un ensemble. Une famille de fonctions $\mathcal{H}$ de S dans $\{0,1\}^n$ est dite ε-AXU$_2$ si, pour tous $x, x' \in S, x \neq x'$ et tout $y \in \{0,1\}^n$, on a $\Pr\left[h \leftarrow_{\$} \mathcal{H} : h(x) \oplus h(x') = y\right] \leq \varepsilon$. ♦

Remarquons qu'il existe des familles de fonctions ε-AXU$_2$ très efficaces avec $\varepsilon \simeq 2^{-n}$ [Sho96].

4.2.2 Description de la construction r-CLRW

Soit r un entier positif. On définit le TBC $\texttt{CLRW}^{r,E,\mathcal{H}}$ (voir figure 4.3) ayant pour domaine $\{0,1\}^n$, espace des clés $\widetilde{\mathcal{K}} = \mathcal{K}^r \times \mathcal{H}^r$, et espace des tweaks $\mathcal{T}$: pour tous $k = (k_1, \ldots, k_r) \in \mathcal{K}^r$, $h = (h_1, \ldots, h_r) \in \mathcal{H}^r$, $t \in \mathcal{T}$, et $x \in \{0,1\}^n$, soit $\texttt{CLRW}^{r,E,\mathcal{H}}((k,h),t,x)$ défini comme la valeur y_r obtenue récursivement par :

$$\begin{cases} y_0 &= x \\ y_i &= \texttt{LRW}^{E,\mathcal{H}}((k_i,h_i),t,y_{i-1}) \quad \text{pour} \quad 1 \leq i \leq r \ . \end{cases}$$

On note également $\texttt{CLRW}^{r,E,\mathcal{H}}_{k,h} := \texttt{CLRW}^{r,E,\mathcal{H}}((k,h),\cdot,\cdot)$ la fonction qui envoie $(t,x) \in \mathcal{T} \times \{0,1\}^n$ sur $y \in \{0,1\}^n$.

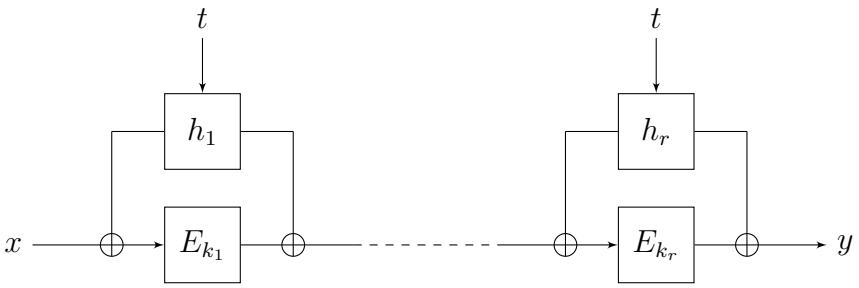

FIGURE 4.3 – Construction du TBC $\texttt{CLRW}^{r,E,\mathcal{H}}$.

Par la suite, nous aurons besoin d'une construction plus idéale où le schéma de chiffrement par blocs E est remplacé par le schéma de chiffrement par blocs parfait E^* sur $\{0,1\}^n$. Le TBC ainsi idéalisé sera noté $\texttt{CLRW}^{r,E^*,\mathcal{H}}$ et, pour chaque $\pi = (\pi_1, \ldots, \pi_r) \in \mathrm{Perm}(n)^r$ et $h = (h_1, \ldots, h_r) \in \mathcal{H}^r$, on notera $\texttt{CLRW}^{r,E^*,\mathcal{H}}_{\pi,h}$ la fonction définie comme $\texttt{CLRW}^{r,E,\mathcal{H}}_{k,h}$ ci-dessus, où les appels à E_{k_i} sont remplacés par des appels à π_i, pour $i = 1..r$ (voir figure 4.4).

Intuitivement, on peut penser que, si E est indistinguable d'une permutation aléatoire (face à une attaque CCA), alors la construction $\texttt{CLRW}^{r,E,\mathcal{H}}$ utilisant E est presque aussi sûre que la construction $\texttt{CLRW}^{r,E^*,\mathcal{H}}$ face à une attaque CCA. Le théorème suivant formalise cette intuition.

Lemme 4.1. *Pour tous q, τ, on a :*

$$\begin{aligned} \mathbf{Adv}^{\widetilde{\text{ncpa}}}_{\texttt{CLRW}^{r,E,\mathcal{H}}}(q,\tau) &\leq r \cdot \mathbf{Adv}^{\text{ncpa}}_{E}(q, \tau + rqT) + \mathbf{Adv}^{\widetilde{\text{ncpa}}}_{\texttt{CLRW}^{r,E^*,\mathcal{H}}}(q,\tau) \\ \mathbf{Adv}^{\widetilde{\text{cca}}}_{\texttt{CLRW}^{r,E,\mathcal{H}}}(q,\tau) &\leq r \cdot \mathbf{Adv}^{\text{cca}}_{E}(q, \tau + rqT) + \mathbf{Adv}^{\widetilde{\text{cca}}}_{\texttt{CLRW}^{r,E^*,\mathcal{H}}}(q,\tau) \ , \end{aligned}$$

où T est le temps de calculs par appels à E ou E^{-1}. ▽

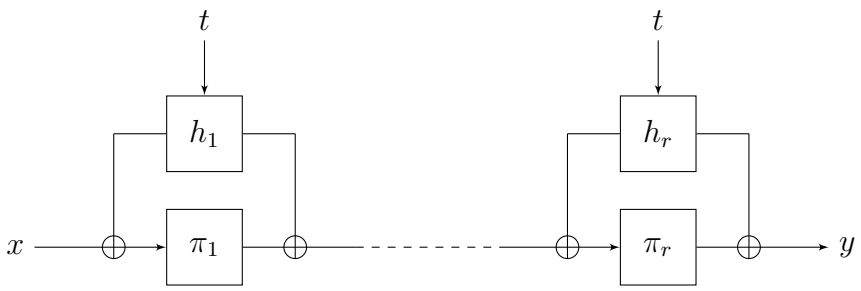

FIGURE 4.4 – Construction du TBC $\texttt{CLRW}^{r,E^*,\mathcal{H}}$.

DÉMONSTRATION. C'est un argument hybride classique. Nous ne prouvons ici que le cas NCPA, le cas CCA étant similaire. Soit $\mathcal{A}$ un attaquant NCPA essayant de distinguer $\texttt{CLRW}^{r,E,\mathcal{H}}$ d'une permutation paramétrable aléatoire. Pour tout $i \in [1; r]$, on considère l'attaquant $\mathcal{A}_i$ essayant de distinguer E d'une permutation aléatoire. $\mathcal{A}_i$ exécute $\mathcal{A}$, répondant à ses requêtes de la manière suivante : il calcule la construction r-CLRW où les $i-1$ premières permutations sont des permutations uniformément aléatoires, la i-ème permutation est calculée en utilisant l'oracle de $\mathcal{A}_i$, et les $r-i$ dernières permutations correspondent à E avec des clés uniformément aléatoires. Notons que $\mathcal{A}_i$ est non adaptatif, fait au plus q requêtes à son propre oracle, et s'exécute en temps au plus $\tau + rqT$. Notons $\mathcal{O}_i$ l'oracle défini comme la construction r-CLRW où les i premières permutations sont uniformément aléatoires, et les $r-i$ dernières permutations sont $r-i$ schémas E avec des clés uniformément aléatoires. Alors, quand $\mathcal{A}_i$ interagit avec une permutation aléatoire, il répond aux requêtes de $\mathcal{A}$ comme l'oracle $\mathcal{O}_{i+1}$, tandis que, lorsqu'il interagit avec E, il répond comme l'oracle $\mathcal{O}_i$. De plus $\mathcal{O}_0 = \texttt{CLRW}^{r,E,\mathcal{H}}$ et $\mathcal{O}_r = \texttt{CLRW}^{r,E^*,\mathcal{H}}$. En utilisant l'inégalité triangulaire, on a :

$$\left|\Pr\left[\mathcal{A}^{\texttt{CLRW}^{r,E,\mathcal{H}}} \Rightarrow 1\right] - \Pr\left[\mathcal{A}^{\widetilde{\pi}} \Rightarrow 1\right]\right| \leq \sum_{i=0}^{r-1} \left|\Pr\left[\mathcal{A}^{\mathcal{O}_i} \Rightarrow 1\right] - \Pr\left[\mathcal{A}^{\mathcal{O}_{i+1}} \Rightarrow 1\right]\right| + \left|\Pr\left[\mathcal{A}^{\texttt{CLRW}^{r,E^*,\mathcal{H}}} \Rightarrow 1\right] - \Pr\left[\mathcal{A}^{\widetilde{\pi}} \Rightarrow 1\right]\right| \quad . \quad \blacksquare$$

Les r premiers termes sont exactement les avantages des attaquants $\mathcal{A}_i$, qui sont tous majorés par $\mathbf{Adv}_E^{\text{ncpa}}(q, \tau + rqT)$. Ce qui prouve le lemme.

Ainsi, l'étude de la sécurité de $\texttt{CLRW}^{r,E,\mathcal{H}}$ se réduit à l'étude de la sécurité de $\texttt{CLRW}^{r,E^*,\mathcal{H}}$ si E est indistinguable d'une permutation aléatoire. Dorénavant, nous allons étudier la sécurité de $\texttt{CLRW}^{r,E^*,\mathcal{H}}$

4.3 Indistinguabilité du schéma r-CLRW face à une attaque NCPA

Nous prouvons ici le théorème suivant :

Théorème 4.2. *Soit $\mathcal{K}, \mathcal{T}$ des ensembles, $E \in \mathsf{BC}(\mathcal{K}, n)$ un schéma de chiffrement par blocs, et $\mathcal{H}$ une famille de fonctions ε-AXU$_2$ de $\mathcal{T}$ dans $\{0,1\}^n$. Alors :*

$$\mathbf{Adv}^{\widetilde{\text{ncpa}}}_{\texttt{CLRW}^{r,E,\mathcal{H}}}(q,\tau) \leq r \cdot \mathbf{Adv}^{\text{ncpa}}_{E}(q, \tau + rqT) + \frac{q^{r+1}}{r+1}(2\varepsilon)^r \ ,$$

où T est le temps de calcul d'un appel à E ou E^{-1}. ♢

En utilisant une famille de fonctions ε-AXU$_2$ où $\varepsilon \simeq 2^{-n}$, on voit que la sécurité atteint $\mathcal{O}(N^{r/(r+1)})$ requêtes (en supposant E suffisamment NCPA sûr). Le lemme 4.1 implique que le théorème précédent est vrai si $\mathbf{Adv}^{\widetilde{\text{ncpa}}}_{\texttt{CLRW}^{r,E^*,\mathcal{H}}}(q,\tau) \leq \frac{q^{r+1}}{r+1}(2\varepsilon)^r$. C'est ce que nous allons prouver.

4.3.1 Avantage NCPA majoré par la distance statistique (étape 1)

On utilise, comme précédemment, la stratégie de preuve par coupling. On commence par transposer le problème du calcul de l'avantage à un calcul de distance statistique. Soit donc un attaquant NCPA $\mathcal{A}$ qui choisit q requêtes à l'avance. Notons (t_i, x_i) la i-ème requête pour tout $i = 1..q$, μ_q la distribution des sorties quand le distingueur $\mathcal{A}$ interagit avec le schéma $\texttt{CLRW}^{r,E^*,\mathcal{H}}$ (la distribution est définie sur l'aléa des tirages uniformes de $\pi = (\pi_1, \ldots, \pi_r) \in \text{Perm}(n)^r$ et $h = (h_1, \ldots, h_r) \in \mathcal{H}^r$) et μ_0 la distribution des sorties quand le distingueur $\mathcal{A}$ interagit avec une permutation paramétrable uniformément aléatoire $\widetilde{\pi}$. Ainsi, pour tout τ (puisque l'inégalité reste vraie pour des attaquant ayant une capacité de calculs non bornée) :

$$\mathbf{Adv}^{\widetilde{\text{ncpa}}}_{\texttt{CLRW}^{r,E^*,\mathcal{H}}}(q,\tau) \leq \|\mu_q - \mu_0\| \ .$$

Par la suite, nous noterons $\tau = +\infty$ dans la formule de l'avantage quand le résultat s'applique aux attaquant ayant une capacité de calculs non bornée.

4.3.2 Diviser pour mieux régner (étape 2)

Pour tout $t \in \mathcal{T}$, soit I_t l'ensemble des indices $i \in [1; q]$ tels que $t_i = t$ et soit $(u_i)_{i \in I_t}$ des éléments de $\mathcal{I}_n$ uniformément aléatoires et deux à deux distincts. Alors la distribution des images de $(t_1, u_1), \ldots, (t_q, u_q)$ par n'importe quelle permutation paramétrable $\widetilde{\pi}'$ indépendante de la distribution des (u_i) est la distribution μ_0, *i.e.* la distribution des images de (t_i, x_i) par une permutation paramétrable uniformément aléatoire $\widetilde{\pi}$. En effet, pour tout t, les valeurs $(\widetilde{\pi}(t_i, x_i))_{i \in I_t}$ et $(\widetilde{\pi}'(t_i, u_i))_{i \in I_t}$ sont, toutes deux, uniformément aléatoires et deux à deux distincts. Remarquons que, pour $(\widetilde{\pi}(t_i, x_i))_{i \in I_t}$, l'aléa provient de $\widetilde{\pi}$ tandis que, pour $(\widetilde{\pi}'(t_i, u_i))_{i \in I_t}$, l'aléa provient des u_i.

Avec cette nouvelle description de μ_0, nous pouvons introduire des distributions intermédiaires qui vont diviser la majoration de $\|\mu_q - \mu_0\|$ en q majorations plus simples à étudier. Pour tout $\ell \in [0; q]$, soit $((t_1, z_1), \ldots, (t_q, z_q))$ un uplet de requêtes telles que $z_i = x_i$ pour $i \leq \ell$, et z_i est uniformément aléatoire dans $\{0,1\}^n \setminus \{z_j \,|\, t_j = t_i, j < i\}$ pour $i > \ell$. Cela signifie que les ℓ premières requêtes sont les requêtes de l'adversaire et les requêtes restantes z_i sont choisies uniformément aléatoires parmi les valeurs possibles (toutes les requêtes doivent être choisies deux à deux distinctes). Notons μ_ℓ la distribution du uplet des q sorties quand une instance aléatoire de $\texttt{CLRW}^{r,E^*,\mathcal{H}}$ reçoit les entrées

$((t_1, z_1), \ldots, (t_q, z_q))$. Alors :

$$\mathbf{Adv}^{\widetilde{\text{ncpa}}}_{\texttt{CLRW}^{r,E^*,\mathcal{H}}}(q, \tau = +\infty) \leq \|\mu_q - \mu_0\| \leq \sum_{\ell=0}^{q-1} \|\mu_{\ell+1} - \mu_\ell\| \ . \tag{4.1}$$

Il reste alors à majorer la distance statistique entre $\mu_{\ell+1}$ et μ_ℓ, pour tout $\ell \in [0; q-1]$. Pour cela, toujours en suivant la même stratégie, nous allons construire un coupling des deux distributions. Remarquons que nous n'avons qu'à considérer les $\ell+1$ premiers éléments des deux uplets de sorties puisque, pour les deux distributions, les i-èmes sorties sont uniformément aléatoires pour $i > \ell+1$. Ainsi :

$$\|\mu_{\ell+1} - \mu_\ell\| = \|\mu'_{\ell+1} - \mu'_\ell\| \ , \tag{4.2}$$

où $\mu'_{\ell+1}$ et μ'_ℓ sont les distributions respectives des $\ell+1$ premières sorties de la construction r-CLRW. Ce résultat est assez intuitif mais la preuve est assez technique (voir [MRS09, Lemme 2]). Nous présentons cette preuve pour le schéma KAF au lemme 5.8.

4.3.3 Coupler les deux distributions adjacentes (étape 3)

Pour définir le coupling de $\mu'_{\ell+1}$ et μ'_ℓ, on considère un $\texttt{CLRW}^{r,E^*,\mathcal{H}}_{\pi,h}$ uniformément aléatoire (*i.e.* $\pi = (\pi_1, \ldots, \pi_r)$ et $h = (h_1, \ldots, h_r)$ sont uniformément aléatoires dans, respectivement, $\text{Perm}(n)^r$ et $\mathcal{H}^r$) qui reçoit les entrées (t_j, x_j) pour $j = 1, \ldots, \ell+1$ de sorte que les sorties soient distribuées selon $\mu'_{\ell+1}$, et on considère un autre $\texttt{CLRW}^{r,E^*,\mathcal{H}}_{\pi',h'}$ uniformément aléatoire (*i.e.* $\pi' = (\pi'_1, \ldots, \pi'_r)$ et $h' = (h'_1, \ldots, h'_r)$ sont uniformément aléatoires dans, respectivement, $\text{Perm}(n)^r$ et $\mathcal{H}^r$) qui reçoit les entrées (t_j, z_j) pour $j = 1, \ldots, \ell+1$ avec $z_j = x_j$ pour tout $j \leq \ell$ et $z_{\ell+1}$ est tiré uniformément aléatoire dans $\{0,1\}^n \setminus \{x_j \,|\, t_j = t_{\ell+1}, j < \ell+1\}$, de sorte que les sorties suivent la distribution μ'_ℓ.

Notation

Pour tout $j \leq \ell+1$ et tout $i \in [0; r]$, on note x_j^i et z_j^i les valeurs définies récursivement par :

$$\left\{ \begin{array}{rcl} x_j^0 & = & x_j, z_j^0 = z_j \\ x_j^{i+1} & = & h_i(t_j) \oplus \pi_i(x_j^i \oplus h_i(t_j)) \\ z_j^{i+1} & = & h'_i(t_j) \oplus \pi'_i(z_j^i \oplus h'_i(t_j)) \ . \end{array} \right. \tag{4.3}$$

Pour pouvoir appliquer le lemme du coupling (lemme 2.1), nous devons corréler (π, h) et (π', h') pour que les sorties des deux systèmes $(x_1^r, \ldots, x_{\ell+1}^r)$ et $(z_1^r, \ldots, z_{\ell+1}^r)$ soient égales avec une grande probabilité. On choisit (π, h) uniformément aléatoire et nous allons construire (π', h') en fonction de (π, h). Il est important de faire attention à la distribution de (π', h'), qui doit rester uniforme pour que $(z_1^r, \ldots, z_{\ell+1}^r)$ suivent bien la distribution μ'_ℓ.

Coupling des ℓ premières requêtes

Pour tout $j \leq \ell$, les j-èmes requêtes x_j^0 et z_j^0 sont égales par définition. Considérons le système (4.3) et fixons $h' = h$ et $\pi'_i(x_j^i \oplus h_i(t_j)) = \pi_i(x_j^i \oplus h_i(t_j))$ pour tous $j \leq \ell$ et $i \leq r$. Cela implique que les ℓ premières sorties $(x_1^r, \ldots, x_\ell^r)$ et $(z_1^r, \ldots, z_\ell^r)$ sont égales.

Coupling de la $(\ell+1)$-ème requête

Pour tout $i \in [0; r-1]$, on définit le coupling de la $\ell+1$-ème requête de la façon suivante :

(1) si il existe $j \leq \ell$ tel que $z^i_{\ell+1} \oplus h_i(t_{\ell+1}) = z^i_j \oplus h_i(t_j)$ alors $\pi'_i(z^i_{\ell+1} \oplus h_i(t_{\ell+1}))$ est déjà défini. A moins que nous ayons couplé $z^i_{\ell+1}$ et $x^i_{\ell+1}$ dans un tour précédent, on ne peut coupler $z^{i+1}_{\ell+1}$ et $x^{i+1}_{\ell+1}$ à ce tour.

(2) sinon, si $z^i_{\ell+1} \oplus h_i(t_{\ell+1}) \neq z^i_j \oplus h_i(t_j)$ pour tout $j \leq \ell$, alors :

   (a) si il existe $j \leq \ell$ tel que $x^i_{\ell+1} \oplus h_i(t_{\ell+1}) = x^i_j \oplus h_i(t_j)$ alors on choisit $\pi'_i(z^i_{\ell+1} \oplus h_i(t_{\ell+1}))$ uniformément aléatoire dans $\{0,1\}^n \setminus \{\pi'_i(z^i_j \oplus h_i(t_j)), j \leq \ell\}$. On ne peut pas coupler $z^{i+1}_{\ell+1}$ et $x^{i+1}_{\ell+1}$ à ce tour.

   (b) sinon, on définit $\pi'_i(z^i_{\ell+1} \oplus h_i(t_{\ell+1})) = \pi_i(x^i_{\ell+1} \oplus h_i(t_{\ell+1}))$. Cela implique que $z^{i+1}_{\ell+1} = x^{i+1}_{\ell+1}$.

Remarquons que lorsque $z^{i+1}_{\ell+1} = x^{i+1}_{\ell+1}$ alors $z^{i'}_{\ell+1} = x^{i'}_{\ell+1}$ pour n'importe quel tour $i' \geq i+1$, en particulier pour $i' = r$, de telle façon que le coupling est réussi pour cette requête.

Vérification que (π', h') est uniformément aléatoire

On a fixé $h' = h$ et h est uniformément aléatoire donc h' est uniformément aléatoire. Pendant le coupling des ℓ premières requêtes, on a fixé $\pi'_i(x^i_j \oplus h_i(t_j)) = \pi_i(x^i_j \oplus h_i(t_j))$ pour tous $j \leq \ell$ et $i \leq r$, et $\pi_i(x^i_j \oplus h_i(t_j))$ est uniformément aléatoire parmi les valeurs possibles donc $\pi'_i(x^i_j \oplus h_i(t_j))$ est uniformément aléatoire parmi les valeurs possibles. La règle (1) dit que, si il y a une collision avec une requête précédente de π'_i, alors on ne peut choisir la valeur de $\pi'_i(z^i_j \oplus h_i(t_j))$, ce qui ne modifie pas la distribution de π'_i. Quand les conditions de la règle (2)(a) sont remplies, il existe un certain $j \leq \ell$ vérifiant :

$$\begin{cases} \pi_i(x^i_{\ell+1} \oplus h_i(t_{\ell+1})) = \pi_i(x^i_j \oplus h_i(t_j)) = \pi'_i(z^i_j \oplus h_i(t_j)) \\ z^i_{\ell+1} \oplus h_i(t_{\ell+1}) \neq z^i_j \oplus h_i(t_j) \ , \end{cases}$$

ce qui implique que $\pi'_i(z^i_{\ell+1} \oplus h_i(t_{\ell+1})) \neq \pi_i(x^i_j \oplus h_i(t_j))$. Ainsi, le coupling est impossible et on choisit $\pi'_i(z^i_{\ell+1} \oplus h_i(t_{\ell+1}))$ uniformément aléatoire parmi les valeurs possibles pour maintenir la distribution de π'_i uniformément aléatoire. Quand les conditions de la règle (2)(b) sont remplies, il n'y a aucun problème pour coupler : $\pi_i(x^i_{\ell+1} \oplus h_i(t_{\ell+1}))$ et $\pi'_i(z^i_{\ell+1} \oplus h_i(t_{\ell+1}))$ sont tous les deux uniformément aléatoires parmi les valeurs possibles. Ainsi, les permutations π'_i sont uniformément aléatoires et indépendantes, comme souhaité, et $(z^r_1, \ldots, z^r_{\ell+1})$ suit la distribution μ'_ℓ.

4.3.4 Majorer la probabilité de ne pas coupler (étape 4)

Il reste à majorer la probabilité de ne pas coupler, *i.e.*

$$(z^r_1, \ldots, z^r_{\ell+1}) \neq (x^r_1, \ldots, x^r_{\ell+1}) \ .$$

Pour tout $i \in [0; r-1]$, notons $\texttt{fail}^i$ l'événement qu'il existe $j \leq \ell$ tel que $z^i_{\ell+1} \oplus h_i(t_{\ell+1}) = z^i_j \oplus h_i(t_j)$ ou $x^i_{\ell+1} \oplus h_i(t_{\ell+1}) = x^i_j \oplus h_i(t_j)$. C'est l'événement de ne pas réussir à coupler

au tour i. On a alors :

$$\begin{aligned}\Pr\left[\texttt{fail}^i\right] &\leq \sum_{j\leq\ell}\Pr\Big[z^i_{\ell+1}\oplus h_i(t_{\ell+1}) = z^i_j\oplus h_i(t_j)\\ &\qquad\qquad\qquad\qquad \text{ou } x^i_{\ell+1}\oplus h_i(t_{\ell+1}) = x^i_j\oplus h_i(t_j)\Big]\\ &= \sum_{j\leq\ell}\Pr\Big[h_i(t_j)\oplus h_i(t_{\ell+1}) = z^i_j\oplus z^i_{\ell+1}\\ &\qquad\qquad\qquad\qquad \text{ou } h_i(t_j)\oplus h_i(t_{\ell+1}) = x^i_j\oplus x^i_{\ell+1}\Big]\\ &\leq \sum_{j\leq\ell} 2\varepsilon = 2\ell\varepsilon\ ,\end{aligned}$$

où la seconde inégalité vient de la propriété ε-AXU$_2$ de $\mathcal{H}$. Remarquons que, quand $t_{\ell+1} = t_j$, alors, nécessairement $z^i_{\ell+1}\neq z^i_j$ et $x^i_{\ell+1}\neq x^i_j$ puisque toutes les requêtes doivent être distinctes, et la probabilité est donc nulle. Puisque les fonctions h_i sont indépendantes, on a :

$$\Pr\left[\bigcap_{i=0}^{r-1}\texttt{fail}^i\right] \leq (2\ell\varepsilon)^r\ . \tag{4.4}$$

En utilisant le lemme du coupling et le fait que $z^r_j = x^r_j$ pour tout $j\leq\ell$, on a :

$$\|\mu'_{\ell+1}-\mu'_\ell\| \leq \Pr\left[(z^r_1,\ldots,z^r_{\ell+1})\neq(x^r_1,\ldots,x^r_{\ell+1})\right] \leq \Pr\left[z^r_{\ell+1}\neq x^r_{\ell+1}\right]\ . \tag{4.5}$$

Si on réussit à coupler la dernière requête à un tour $i\leq r-1$, on sait que $z^{i'}_{\ell+1}$ et $x^{i'}_{\ell+1}$ restent égaux dans les tours suivants donc :

$$\Pr\left[z^r_{\ell+1}\neq x^r_{\ell+1}\right] \leq \Pr\left[\bigcap_{i=0}^{r-1}\texttt{fail}^i\right]\ . \tag{4.6}$$

Et, en utilisant (4.4), (4.5) et (4.6), on a :

$$\|\mu'_{\ell+1}-\mu'_\ell\| \leq (2\ell\varepsilon)^r\ . \tag{4.7}$$

4.3.5 En déduire un majorant de l'avantage NCPA (étape 5)

En utilisant les équations (4.1), (4.2) et (4.7), on obtient que :

$$\begin{aligned}\mathbf{Adv}^{\widetilde{\text{ncpa}}}_{\texttt{CLRW}^{r,E^*,\mathcal{H}}}(q,\tau=+\infty) &\leq \sum_{\ell=0}^{q-1}\|\mu'_{\ell+1}-\mu'_\ell\|\\ &\leq \sum_{\ell=0}^{q-1}(2\ell\varepsilon)^r\\ &\leq \int_0^q (2\ell\varepsilon)^r dl\\ &= \frac{q^{r+1}}{r+1}(2\varepsilon)^r\ .\end{aligned}$$

L'inégalité ci-dessus combinée au lemme 4.1 permet de prouver le théorème 4.2, c'est-à-dire :

$$\mathbf{Adv}^{\widetilde{\text{ncpa}}}_{\texttt{CLRW}^{r,E,\mathcal{H}}}(q,\tau) \leq r\cdot\mathbf{Adv}^{\text{ncpa}}_E(q,\tau+rqT) + \frac{q^{r+1}}{r+1}(2\varepsilon)^r\ ,$$

4.4 Indistinguabilité du schéma r-CLRW face à une attaque CCA

Dans cette section, nous commençons par prouver un théorème général de composition pour les schémas de chiffrement par blocs paramétrables. Ce théorème est du type « two weak make one strong » qui consiste à composer deux schémas de chiffrement par blocs NCPA sûrs pour obtenir un schéma de chiffrement par blocs CCA sûr, comme l'ont étudié Maurer, Renner et Pietrzak [MP04, MPR07] et Cogliati, Patarin et Seurin [CPS14]. Nous prouvons le même résultat pour les TBCs avec la particularité que, dans la composition, les tweaks doivent être similaires dans les deux schémas pour composer « proprement ». Le théorème que nous prouvons se place dans la cadre de la théorie de l'information (c'est-à-dire pour des attaquants avec une capacité de calculs non-bornée) et nous appliquons ce théorème à la construction $\texttt{CLRW}^{r,E^*\mathcal{H}}$. Comme nous l'avons fait pour la preuve d'indistinguabilité du schéma d'Even-Mansour itéré, nous utilisons la théorie des Coefficients H de Jacques Patarin [Pat91, Pat08] pour prouver ce théorème de composition. Nous pourrions probablement utiliser le formalisme des systèmes aléatoires [Mau02] pour obtenir une borne optimale comme dans [MPR07], néanmoins, des problèmes subtils ont été trouvés dans cette technique de preuve et nous préférons donc l'approche plus simple utilisant les Coefficients H. Nous déduirons de ce théorème la sécurité de r-CLRW face à une attaque CCA utilisant jusqu'à $\mathcal{O}(2^{rn/(r+2)})$ requêtes.

4.4.1 Définitions et résultats préliminaires

Fixons $\widetilde{E} \in \mathsf{TBC}(\mathcal{K}, \mathcal{T}, \mathcal{D})$. Pour tout $t = (t_1, \ldots, t_q) \in \mathcal{T}^q$, et tout $x = (x_1, \ldots, x_q) \in \Omega_t$, on note $\nu_{(t,x)}$ la distribution sur Ω_t induite par $\widetilde{E}$ et $\nu^*_{(t,x)}$ la distribution induite par une permutation paramétrable aléatoire sur les entrées (t_i, x_i), c'est-à-dire pour $y = (y_1, \ldots, y_q) \in \Omega_t$:

$$\begin{cases} \nu_{(t,x)}(y) &= \Pr\left[k \leftarrow_\$ \mathcal{K} : \widetilde{E}_k(t_i, x_i) = y_i, \forall i \leq q\right] \\ \nu^*_{(t,x)}(y) &= \Pr\left[\widetilde{\pi} \leftarrow_\$ \mathsf{BC}(\mathcal{T}, \mathcal{D}) : \widetilde{\pi}(t_i, x_i) = y_i, \forall i \leq q\right] \ . \end{cases}$$

Remarquons que $\nu^*_{(t,x)}$ est la distribution uniforme sur Ω_t. Pour tout $\alpha \in [0,1]$, on note $S_{\alpha,(t,x)}$ l'ensemble des $y \in \Omega_t$ vérifiant $\nu_{(t,x)}(y) \geq (1-\alpha)\nu^*_{(t,x)}(y)$.

Nous commençons par prouver deux lemmes qui seront utiles pour notre résultat principal. Le premier établit que, si pour tous $t = (t_1, \ldots, t_q)$, $x = (x_1, \ldots, x_q)$, et $y = (y_1, \ldots, y_q)$, la probabilité que $\widetilde{E}_k$ envoie (t_i, x_i) sur y_i pour tout i est proche de la probabilité correspondante pour une permutation paramétrable aléatoire, alors l'avantage de n'importe quel attaquant CCA pour distinguer $\widetilde{E}$ d'une permutation aléatoire uniforme, avec q requêtes, est faible.

Lemme 4.3. *Soit $\widetilde{E} \in \mathsf{TBC}(\mathcal{K}, \mathcal{T}, \mathcal{D})$, et $q \leq |\mathcal{D}|$. Si il existe $\alpha \in [0,1]$ tel que, pour tout $t \in \mathcal{T}^q$ et pour tout $x \in \Omega_t$, $\nu^*_{(t,x)}(S_{\alpha,(t,x)}) = 1$, alors :*

$$\mathbf{Adv}^{\widetilde{\mathrm{cca}}}_{\widetilde{E}}(q, \tau = +\infty) \leq \alpha \ . \qquad \triangledown$$

Démonstration. Considérons un attaquant CCA $\mathcal{A}$, avec une capacité de calculs non bornée, faisant q requêtes à un oracle $\mathcal{O}$ qui se comporte comme $\widetilde{E}$ ou comme une permutation paramétrable aléatoire $\widetilde{\pi}$. On suppose, sans perte de généralité, que $\mathcal{A}$ est déterministe. Notons $\delta = (\delta_1, \ldots, \delta_q) \in \mathcal{D}^q$ la transcription de l'attaque définie comme suit. Si $\mathcal{A}$ fait une requête directe (t_1, x_1) et reçoit une réponse y_1, on a $\delta_1 = y_1$ et alors, l'attaquant continue son attaque en recevant les réponses suivantes $\delta_2, \ldots, \delta_q$. Si l'attaquant fait une requête inverse (t_i, y_i) alors δ_i est la réponse x_i. Pour toute transcription δ, on note $t(\delta), x(\delta)$ et $y(\delta)$ les valeurs correspondantes de $t_1, \ldots, t_q, x_1, \ldots, x_q, y_1, \ldots, y_q$. On note Σ l'ensemble des transcriptions δ telles que l'attaquant réponde 1 à la fin de l'attaque. Si l'oracle se comporte comme $\widetilde{E}$ alors la probabilité que l'attaquant réponde 1 est exactement

$$\sum_{\delta \in \Sigma} \nu_{t(\delta),x(\delta)}(y(\delta)) \ .$$

Si l'oracle se comporte comme une permutation paramétrable aléatoire $\widetilde{\pi}$ alors la probabilité que l'attaquant réponde 1 est exactement

$$\sum_{\delta \in \Sigma} \nu^*_{t(\delta),x(\delta)}(y(\delta)) \ .$$

On en déduit que l'avantage de $\mathcal{A}$ est égal à :

$$\left| \sum_{\delta \in \Sigma} \left(\nu_{t(\delta),x(\delta)}(y(\delta)) - \nu^*_{t(\delta),x(\delta)}(y(\delta)) \right) \right| \ . \tag{4.8}$$

Puisque, pour tous $t \in \mathcal{T}^q$, $x \in \Omega_t$, et $y \in \Omega_t$, on a $\nu_{(t,x)}(y) \geq (1-\alpha)\nu^*_{(t,x)}(y)$, on en déduit que :

$$\begin{aligned} \sum_{\delta \in \Sigma} \left(\nu_{t(\delta),x(\delta)}(y(\delta)) - \nu^*_{t(\delta),x(\delta)}(y(\delta)) \right) &\geq -\alpha \\ \text{et} \quad \sum_{\delta \notin \Sigma} \left(\nu_{t(\delta),x(\delta)}(y(\delta)) - \nu^*_{t(\delta),x(\delta)}(y(\delta)) \right) &\geq -\alpha \ . \end{aligned} \tag{4.9}$$

Finalement, on vérifie que :

$$\begin{aligned} \sum_{\delta \in \Sigma} \left(\nu_{t(\delta),x(\delta)}(y(\delta)) - \nu^*_{t(\delta),x(\delta)}(y(\delta)) \right) = \\ - \sum_{\delta \notin \Sigma} \left(\nu_{t(\delta),x(\delta)}(y(\delta)) - \nu^*_{t(\delta),x(\delta)}(y(\delta)) \right) \end{aligned} \tag{4.10}$$

car

$$\sum_{\delta} \nu_{t(\delta),x(\delta)}(y(\delta)) = \sum_{\delta} \nu^*_{t(\delta),x(\delta)}(y(\delta)) = 1 \ .$$

En utilisant les équations (4.8), (4.9) et (4.10), on déduit que l'avantage de $\mathcal{A}$ est majoré par α. ∎

Le deuxième lemme établit que, si l'avantage du meilleur attaquant NCPA est petit, alors, pour tous t, x, presque tous les y sont tels que la probabilité d'envoyer (t, x) sur y, pour un $\widetilde{E}_k$ aléatoire, est proche de la probabilité d'envoyer (t, x) sur y pour une permutation paramétrable aléatoire.

Lemme 4.4. *Soit $\widetilde{E} \in \mathsf{TBC}(\mathcal{K}, \mathcal{T}, \mathcal{D})$ et $q \leq |\mathcal{D}|$. Si il existe $\beta \in [0,1]$ tel que*

$$\mathbf{Adv}^{\widetilde{\mathrm{ncpa}}}_{\widetilde{E}}(q, \tau = +\infty) \leq \beta \ ,$$

alors, pour tous $t \in \mathcal{T}^q$ et $x \in \Omega_t$, on a :

$$\nu^*_{(t,x)}\left(S_{\sqrt{\beta},(t,x)}\right) \geq 1 - \sqrt{\beta} \ . \qquad \triangledown$$

Démonstration. Par contraposée, supposons qu'il existe $t = (t_1, \ldots, t_q) \in \mathcal{T}^q$ et $x = (x_1, \ldots, x_q) \in \Omega_t$ tels que

$$\nu^*_{(t,x)}\left(S_{\sqrt{\beta},(t,x)}\right) < 1 - \sqrt{\beta} \ .$$

Considérons l'attaquant qui envoie les requêtes (t_1, x_1), $\ldots$, (t_q, x_q) et répond 0 si les réponses $y = (y_1, \ldots, y_q)$ sont telles que $y \in S_{\sqrt{\beta},(t,x)}$ et 1 sinon. Son avantage est exactement

$$\left| \sum_{y \notin S_{\sqrt{\beta},(t,x)}} \nu_{(t,x)}(y) - \nu^*_{(t,x)}(y) \right| \ ,$$

et $y \notin S_{\sqrt{\beta},(t,x)}$ signifie que, par définition, $\nu_{(t,x)}(y) < (1 - \sqrt{\beta})\nu^*_{(t,x)}(y)$, de telle façon que l'avantage de cet adversaire est strictement supérieur à :

$$\sqrt{\beta} \times \left(1 - \nu^*_{(t,x)}\left(S_{\sqrt{\beta},(t,x)}\right)\right) > \beta \ ,$$

ce qui prouve le lemme. ■

4.4.2 Un théorème de composition pour les schémas de chiffrement par blocs paramétrables

Étant donnés deux TBS partageant le même ensemble de tweaks et le même domaine $\widetilde{E}_1 \in \mathsf{TBC}(\mathcal{K}_1, \mathcal{T}, \mathcal{D})$ et $\widetilde{E}_2 \in \mathsf{TBC}(\mathcal{K}_2, \mathcal{T}, \mathcal{D})$, on définit le TBC $\widetilde{E}_2 \circ \widetilde{E}_1 \in \mathsf{TBC}(\mathcal{K}_1 \times \mathcal{K}_2, \mathcal{T}, \mathcal{D})$ par :

$$\forall (t,x) \in \mathcal{D} \times \mathcal{T}, (k_1, k_2) \in \mathcal{K}_1 \times \mathcal{K}_2, \quad \widetilde{E}_2 \circ \widetilde{E}_1((k_1,k_2),t,x) := \widetilde{E}_2(k_2, t, \widetilde{E}_1(k_1, t, x)) \ .$$

Théorème 4.5. *Soit $\widetilde{E}_1 \in \mathsf{TBC}(\mathcal{K}_1, \mathcal{T}, \mathcal{D})$ et $\widetilde{E}_2 \in \mathsf{TBC}(\mathcal{K}_2, \mathcal{T}, \mathcal{D})$ deux TBCs vérifiant :*

$$\mathbf{Adv}^{\widetilde{\mathrm{ncpa}}}_{\widetilde{E}_1}(q, \tau = +\infty) \leq \beta_1 \text{ et } \mathbf{Adv}^{\widetilde{\mathrm{ncpa}}}_{\widetilde{E}_2}(q, \tau = +\infty) \leq \beta_2 \ .$$

Alors :

$$\mathbf{Adv}^{\widetilde{\mathrm{cca}}}_{\widetilde{E}_2^{-1} \circ \widetilde{E}_1}(q, \tau = +\infty) \leq 2(\sqrt{\beta_1} + \sqrt{\beta_2}) \ . \qquad \diamondsuit$$

Démonstration. Notons ν^1, ν^2, et ν^3 les distributions associées respectivement à $\widetilde{E}_1, \widetilde{E}_2$ et $\widetilde{E}_2^{-1} \circ \widetilde{E}_1$. Pour tous $t \in \mathcal{T}^q$, $x \in \Omega_t$, et $\alpha \in [0,1]$, on note $S^{\widetilde{E}_i}_{\alpha,(t,x)}$ l'ensemble $S_{\alpha,(t,x)}$ correspondant à $\widetilde{E}_i$, $i = 1, 2$.

Par le lemme 4.4, pour tous $t \in \mathcal{T}^q$, $x \in \Omega_t$, et $y \in \Omega_t$, on a :

$$\nu^*_{(t,x)}\left(S^{\widetilde{E}_1}_{\sqrt{\beta_1},(t,x)}\right) \geq 1 - \sqrt{\beta_1} \quad \text{et} \quad \nu^*_{(t,y)}\left(S^{\widetilde{E}_2}_{\sqrt{\beta_2},(t,y)}\right) \geq 1 - \sqrt{\beta_2} \ . \tag{4.11}$$

De plus, pour tout $(k_1, k_2) \in \mathcal{K}_1 \times \mathcal{K}_2$, $\widetilde{E}_2^{-1} \circ \widetilde{E}_1((k_1,k_2),\cdot,\cdot)$ envoie (t,x) sur y si et seulement si, pour tout $i \leq q$, $\widetilde{E}_1(k_1, t_i, x_i) = \widetilde{E}_2(k_2, t_i, y_i)$. En notant $S' = S^{\widetilde{E}_1}_{\sqrt{\beta_1},(t,x)} \cap S^{\widetilde{E}_2}_{\sqrt{\beta_2},(t,y)}$, on a, pour tout $y \in \Omega_t$:

$$\begin{aligned}
\nu^3_{(t,x)}(y) &= \sum_{z \in \Omega_t} \nu^1_{(t,x)}(z) \cdot \nu^2_{(t,y)}(z) \\
&\geq \sum_{z \in S'} \nu^1_{(t,x)}(z) \cdot \nu^2_{(t,y)}(z) \\
&\geq \sum_{z \in S'} \left(1 - \sqrt{\beta_1}\right) {\nu^*}_{(t,x)}(z) \cdot \left(1 - \sqrt{\beta_2}\right) {\nu^*}_{(t,y)}(z) \\
&\geq \left(1 - \sqrt{\beta_1}\right)\left(1 - \sqrt{\beta_2}\right) \frac{|S'|}{|\Omega_t|^2} \\
&= \left(1 - \sqrt{\beta_1}\right)\left(1 - \sqrt{\beta_2}\right) \nu^*_{(t,x)}(S') \nu^*_{(t,x)}(y) \ .
\end{aligned}$$

Par définition de S' et en utilisant l'équation 4.11, on a $\nu^*_{(t,x)}(S') \geq (1 - \sqrt{\beta_1} - \sqrt{\beta_2})$ (remarquons que ν^* ne dépend finalement que de t), et ainsi :

$$\nu^3_{(t,x)}(y) \geq (1 - 2(\sqrt{\beta_1} + \sqrt{\beta_2})) \nu^*_{(t,x)}(y) \ .$$

Puisque cette inéquation est vraie pour tous t, x, et y, le lemme 4.3, avec $\alpha = 2(\sqrt{\beta_1} + \sqrt{\beta_2})$, permet de conclure. ∎

4.4.3 Application au schéma r-CLRW

Pour finir, nous appliquons le résultat précédent pour prouver la sécurité du schéma r-CLRW face à une attaque CCA.

Théorème 4.6. *Soit $\mathcal{K}, \mathcal{T}$ deux ensembles, $E \in \mathsf{BC}(\mathcal{K}, n)$ un schéma de chiffrement par blocs, et $\mathcal{H}$ une famille de fonctions ε-AXU$_2$ de $\mathcal{T}$ dans $\{0,1\}^n$. Alors, pour tout entier pair r, on a :*

$$\mathbf{Adv}^{\widetilde{\text{cca}}}_{\mathtt{CLRW}^{r,E,\mathcal{H}}}(q,\tau) \leq r \cdot \mathbf{Adv}^{\text{cca}}_{E}(q, \tau + rqT) + \frac{4\sqrt{2}}{\sqrt{r+2}} q^{(r+2)/4} (2\varepsilon)^{r/4} \ ,$$

où T est le temps de calcul d'un appel à E ou E^{-1}. ♢

Démonstration. En notant que l'inverse d'un schéma $r/2$-CLRW est encore un schéma $r/2$-CLRW, on applique le théorème 4.5 pour obtenir :

$$\mathbf{Adv}^{\widetilde{\text{cca}}}_{\mathtt{CLRW}^{r,E^*,\mathcal{H}}}(q, \tau = +\infty) \leq 4\sqrt{\alpha} \ ,$$

où

$$\alpha := \mathbf{Adv}^{\widetilde{\text{ncpa}}}_{\texttt{CLRW}^{r/2},E^*,\mathcal{H}}(q,\tau=+\infty) \leq \frac{q^{r/2+1}}{r/2+1}(2\varepsilon)^{r/2}$$

à l'aide des résultats de la section 4.3. Le lemme 4.1 permet alors de conclure. ∎

A nouveau, en utilisant une famille de fonctions ε-AXU$_2$ avec $\varepsilon \simeq 2^{-n}$, le schéma atteint une sécurité CCA jusqu'à $\mathcal{O}(2^{rn/(r+2)})$ requêtes.

Chapitre 5

Preuve d'indistinguabilité des schémas de Feistel à clés alternées

Dans ce chapitre, nous présentons les schémas de Feistel à clés alternées et nous prouvons leur indistinguabilité à l'aide de la technique du coupling. Cette construction et cette preuve ont été présentées à FSE 2014 [LS14].

5.1 Schéma de Feistel à clés alternées

5.1.1 Les deux structures principales d'un schéma de chiffrement par blocs

Les schémas de chiffrement par blocs se classent principalement en deux structures : les structures de Feistel et les structures dites de « substitution-permutation networks » SPNs (voir figure 5.1).

Les structures de Feistel ont largement été étudiées dans le modèle idéalisé où les fonctions de tours F_i sont supposées uniformément aléatoires et secrètes. Ce cadre est aussi appelé « Luby-Rackoff framework » et un schéma de Feistel où les fonctions internes sont uniformément aléatoires et secrètes est appelé schéma de Luby-Rackoff en référence aux travaux initiateurs de Luby et Rackoff [LR88] qui ont prouvé qu'un schéma de Luby-Rackoff à 3 tours est une permutation pseudo-aléatoire (c'est-à-dire indistinguable d'une permutation aléatoire face à une attaque CPA). Par la suite, Patarin [Pat90] a prouvé que le schéma de Luby-Rackoff à 4 tours est une permutation super pseudo-aléatoire (c'est-à-dire indistinguable d'une permutation aléatoire face à une attaque CCA) et une multitude de travaux ont permis d'améliorer les bornes de sécurité pour un nombre plus élevé de tours [Mau92, MP03, Vau03, Pat04, HR10, Pat10].

Pendant longtemps, les preuves de sécurité pour les structures SPN se limitaient à prouver la résistance face à des attaques bien spécifiques comme les attaques différentielles ou linéaires [DR02]. Néanmoins, récemment, il y a eu de nombreux travaux sur le schéma d'Even-Mansour itéré (voir chapitre 3). Dans ce schéma, les permutations internes sont supposées publiques ce qui est plus réaliste car un attaquant peut effectivement avoir accès aux permutations internes. Cette caractéristique n'a, jusqu'alors, jamais été pleinement considérée pour une structure de Feistel.

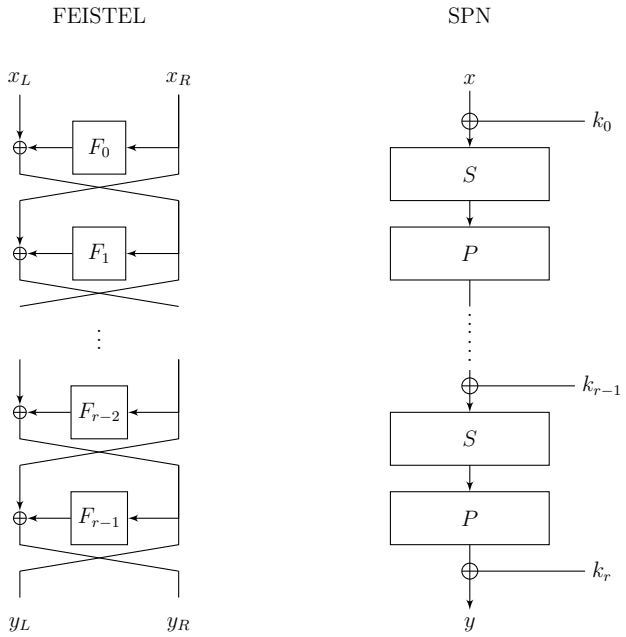

FIGURE 5.1 – Structure de Feistel à r tours et SPN à r tours.

5.1.2 Définition d'un schéma de Feistel à clés alternées

Contrairement au schéma d'Even-Mansour itéré, les fonctions de tours des schémas de Luby-Rackoff sont secrètes et c'est en remarquant que nous pouvions combiner les propriétés des deux schémas que Yannick SEURIN et moi-même avons imaginé le modèle du schéma de Feistel à clés alternées « Key-Alternating Feistel cipher » (KAF) [LS14] (voir figure 5.2). Ce schéma est un schéma de Feistel où les fonctions de tours sont publiques et où l'entrée de la fonction de tour est xorée avec une clé secrète. Plus précisément, un tour d'un schéma KAF est de la forme $(x_L, x_R) \mapsto (x_R, x_L \oplus F(x_R \oplus k))$ où x_L et x_R sont les parties gauche et droite de l'entrée, F une fonction uniformément aléatoire publique et k une clé uniformément aléatoire secrète. Les fonctions de tours sont accessibles à l'attaquant comme une boîte noire (il n'a pas la description interne des fonctions de tours mais il peut faire des requêtes à F). Ce schéma offre donc plus de possibilités à l'attaquant et nous prouvons, là encore à l'aide de la technique du coupling, qu'un KAF à r tours, avec des fonctions internes dans $\mathcal{F}_n$, est indistinguable d'une permutation aléatoire de $\mathcal{P}_{2n}$ jusqu'à un nombre de requêtes en $\mathcal{O}\left(N^{\frac{t}{t+1}}\right)$ où $t = \lfloor \frac{r}{3} \rfloor$ pour une attaque NCPA et $t = \lfloor \frac{r}{6} \rfloor$ pour une attaque CCA, et $N = 2^n$.

Remarquons qu'un KAF à deux tours n'est rien d'autre qu'un schéma d'Even-Mansour à un tour et une clé, où la permutation interne est un schéma de Feistel à 2 tours publique (voir figure 5.3). Ainsi, nous avons nommé ce schéma « Key-Alternating Feistel cipher » en référence au « Key-Alternating cipher » (le schéma d'Even-Mansour itéré).

Dans le cas où l'on interdit à l'attaquant de faire des requêtes aux fonctions internes, on retrouve un schéma de Luby-Rackoff classique (les fonctions internes sont secrètes). Dans ce cadre là, nous avons amélioré les bornes de sécurité de Hoang et Rogaway [HR10] en diminuant d'environ 1/3 le nombre de tours nécessaires pour obtenir une sécurité donnée. Plus précisément, nous montrons qu'un schéma de Luby-Rackoff à r tours est CCA sûr

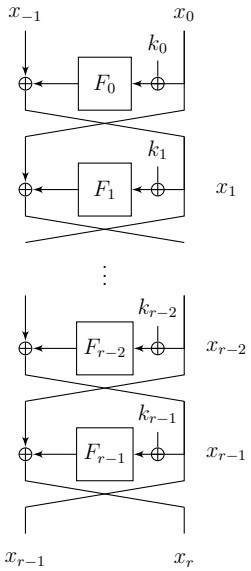

FIGURE 5.2 – Un KAF à r tours.

jusqu'à $\mathcal{O}(N^{\frac{t}{t+1}})$ où $t = \lfloor \frac{r-1}{4} \rfloor$.

5.1.3 Notations et lien entre un KAF et un schéma d'Even-Mansour itéré

Étant donnée une fonction F de $\mathcal{F}_n$ et une clé k de n bits, le schéma de Feistel à clés alternées à 1 tour est la permutation Ψ_k^F de $\mathcal{P}_{2n}$ définie par :

$$\Psi_k^F(x_L, x_R) = (x_R, x_L \oplus F(x_R \oplus k)),$$

où x_L et x_R sont respectivement les parties gauches et droites de l'entrée.

Un schéma de Feistel à clés alternées à r tours (appelé KAF) est caractérisé par r fonctions de tours publiques $F_0, \ldots, F_{r-1}$ de $\mathcal{F}_n$, et sera noté $\mathtt{KAF}^{F_0,\ldots F_{r-1}}$. Son espace des clés est $(\{0,1\}^n)^r$ et son domaine est $\{0,1\}^{2n}$. Il envoie une clé $(k_0, \ldots, k_{r-1})$ et un message x sur le chiffré défini par :

$$\mathtt{KAF}^{F_0,\ldots F_{r-1}}((k_0, \ldots, k_{r-1}), x) = \Psi_{k_{r-1}}^{F_{r-1}} \circ \cdots \circ \Psi_{k_0}^{F_0}(x).$$

Nous noterons $\mathtt{KAF}_{k_0,\ldots,k_{r-1}}^{F_0,\ldots F_{r-1}}$ la permutation de $\mathcal{P}_{2n}$ qui envoie x sur $\mathtt{KAF}^{F_1,\ldots F_r}((k_0, \ldots, k_{r-1}), x)$. Quand le nombre de tours est clair, on note simplement $\boldsymbol{F} = (F_0, \ldots, F_{r-1}), k = (k_0, \ldots, k_{r-1})$, et $\mathtt{KAF}_k^{\boldsymbol{F}}$ la permutation de $\mathcal{P}_{2n}$ caractérisée par les fonctions de tours $\boldsymbol{F}$ et les clés k.

Comme l'ont noté Daemen et Rijmen [DR07], un KAF avec un nombre pair de tours peut être vu comme un cas particulier d'un schéma d'Even-Mansour itéré. En effet, comme nous le voyons sur la figure 5.3, un KAF à 2 tours peut être réécrit comme :

$$\Psi_{k_{i+1}}^{F_{i+1}} \circ \Psi_{k_i}^{F_i}(x) = (k_{i+1} \| k_i) \oplus \Psi_0^{F_{i+1}} \circ \Psi_0^{F_i}((k_{i+1} \| k_i) \oplus x).$$

Ici, $\Psi_0^{F_{i+1}} \circ \Psi_0^{F_i}$ est le schéma de Feistel à 2 tours avec les fonctions de tours F_i et F_{i+1}. Ainsi, cette permutation est publique puisque F_i et F_{i+1} le sont. Rappelons que

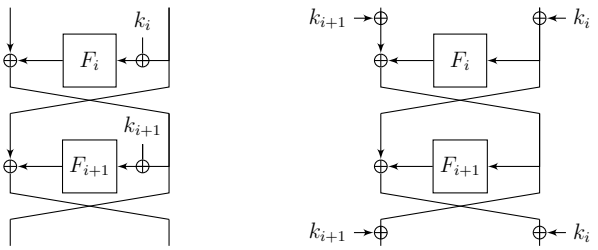

FIGURE 5.3 – Deux façons de voir un KAF à 2 tours.

le schéma d'Even-Mansour à 1 clé sur $2n$ bits est défini par $E(k, x) = k \oplus P(k \oplus x)$, où k est une clé de $2n$ bits, x est le message de $2n$ bits et P est une permutation de $\mathcal{P}_{2n}$ [EM97, DKS12]. Un KAF de $2r'$ tours ayant pour fonctions de tours $(F_0, \ldots, F_{2r'-1})$ et les clés $(k_0, \ldots, k_{2r'-1})$ peut donc être vu comme un schéma d'Even-Mansour itéré à r' tours où la i-ème permutation, $i = 0, \ldots, r' - 1$, est le schéma de Feistel (sans clés) à 2 tours ayant pour fonctions de tours F_{2i} et F_{2i+1}, et la suite de clés de $2n$ bits est $(\tilde{k}_0, \tilde{k}_0 \oplus \tilde{k}_1, \ldots, \tilde{k}_{r'-2} \oplus \tilde{k}_{r'-1}, \tilde{k}_{r'-1})$ avec $\tilde{k}_i = k_{2i+1} \| k_{2i}$.

5.1.4 Travaux connexes

Nous n'avons connaissance que de deux travaux similaires au nôtre. Le premier est un article de Ramzan et Reyzin [RR00] qui montre qu'un schéma de Feistel à 4 tours reste sûr face à une attaque CCA si l'attaquant a accès aux deux fonctions de tours du milieu (il peut faire des requêtes à F_2 et F_3). Le second est un article de Gentry et Ramzan [GR04] qui montre que la permutation interne publique du schéma d'Even-Mansour peut être remplacée par un schéma de Feistel à 4 tours et la construction résultante reste sûre face à une attaque CCA. Bien que leur construction ne nécessite que 4 tours, et 6 pour la nôtre, leur preuve de sécurité donne une borne en $\mathcal{O}(2^{n/2})$ tandis que notre preuve de sécurité donne une borne qui s'améliore asymptotiquement, avec le nombre de tours, vers la borne de la théorie de l'information de $\mathcal{O}(2^n)$ requêtes. Notre résultat est le premier qui dépasse la borne des anniversaires pour les KAFs.

5.2 Lemme probabiliste utile

Dans cette section, on prouve un lemme probabiliste qui est au coeur de la preuve d'indistinguabilité d'un KAF. Toute cette section peut être lue maintenant ou après avoir lu la section suivante sur l'indistinguabilité NCPA d'un KAF. Le résultat que nous allons établir ici ne sera utilisé qu'au moment où nous calculerons la probabilité de coupler, dans les sections suivantes. Étant donné des événements $A_{i_1}, \ldots, A_{i_k}$ définis sur le même espace de probabilité Ω, on notera $A_{i_1} A_{i_2} \cdots A_{i_k}$ l'événement $A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}$. Pour $r \geq 2$, soient $A_1, \ldots, A_r$ des événements définis sur le même espace de probabilité Ω, vérifiant la condition suivante de « dépendance négative » :

Définition 5.1
Soit $p \in]0, 1[$. Une suite d'événements $A_1, \ldots, A_r$ est dite p-négativement dépendante si,

pour tout $i \in [1;r]$ et tout sous-ensemble $S \subseteq [1;i-1]$, on a :

$$\Pr\left[A_i \middle| \bigcap_{j\in S} A_j\right] \leq p\,,$$

avec la convention que l'intersection vide est l'événement certain Ω (ainsi, en particulier $\Pr[A_i] \leq p$ pour $i \in [1;r]$). ♦

On note C_r l'événement $C_r = \cap_{i=1}^{r-1}(A_i \cup A_{i+1})$, c'est-à-dire :

$$C_r = (A_1 \cup A_2)(A_2 \cup A_3)\cdots(A_{r-2} \cup A_{r-1})(A_{r-1} \cup A_r)\,.$$

Notre objectif est de trouver un bon majorant de la probabilité de l'événement C_r (nous verrons dans la section suivante que cet événement est lié à la probabilité de ne pas coupler, et donc à l'avantage). Remarquons que l'événement C_r est une intersection d'événements, ce qui ne permet pas, au premier abord, de trouver facilement une majoration. Néanmoins, en développant C_r sous la forme d'unions d'événements, on peut facilement majorer la probabilité de C_r à l'aide du simple lemme suivant :

Lemme 5.1. *Soit $A_1, \ldots, A_r$ une suite p-négativement dépendante. Alors, pour tout $k \in [1;r]$ et toute suite d'entiers deux à deux distincts $i_1, \ldots, i_k$ dans $[1;r]$:*

$$\Pr\left[A_{i_1} \cdots A_{i_k}\right] \leq p^k\,. \qquad \triangledown$$

Démonstration. Par récurrence sur k. ■

Pour une suite $\alpha \in \{0,1\}^{r-1}$, notons α_i le i-ème bit de α. En développant l'événement C_r, on obtient l'expression :

Lemme 5.2.

$$\bigcap_{i=1}^{r-1}(A_i \cup A_{i+1}) = \bigcup_{\alpha\in\{0,1\}^{r-1}} \bigcap_{i=1}^{r-1} A_{i+\alpha_i}\,. \qquad \triangledown$$

Démonstration. Par récurrence sur r. ■

Pour toute suite $\alpha \in \{0,1\}^{r-1}$, notons $B_{r,\alpha} = \cap_{i=1}^{r-1} A_{i+\alpha_i}$, de telle façon que $C_r = \cup_{\alpha\in\{0,1\}^{r-1}} B_{r,\alpha}$. En fonction de α, $B_{r,\alpha}$ peut être l'intersection d'un nombre d'événements strictement inférieur à $r-1$ (par exemple, quand $\alpha_i = 1$ et $\alpha_{i+1} = 0$ pour un certain i). De plus, pour deux suites distinctes α et α', il est possible que $B_{r,\alpha} \subset B_{r,\alpha'}$. Considérons par exemple le cas $r = 3$. Alors $B_{3,00} = A_1 \cap A_2$ et $B_{3,10} = A_2 \cap A_2 = A_2$, et donc $B_{3,00} \subset B_{3,10}$ (voir table 5.1 pour la forme développée et la forme « réduite » de C_r pour r jusqu'à $r = 8$). Cela motive la définition suivante de suites *irréductibles* :

Définition 5.2
On définit l'ensemble des suites *irréductibles* comme le langage régulier suivant, λ étant la chaîne vide :

$$\mathcal{I} = \{\lambda, 0\}\{10, 100\}^*\{\lambda, 1\}\,.$$

Ainsi, les suites irréductibles sont obtenues en concaténant possiblement un 0, puis les motifs 10 et 100 de manière arbitraire, et possiblement un 1 pour terminer la suite. Les suites dans $\{0,1\}^* \setminus \mathcal{I}$ sont appelées *réductibles*. On note $\mathcal{I}_r$ l'ensemble des suites irréductibles de longueur r. ♦

Il est facile de voir que les suites irréductibles sont exactement les suites α telles que 0α ne contient pas trois zéros consécutifs ou deux zéros consécutifs, mais nous n'aurons pas besoin de cette caractérisation par la suite.

L'utilité des suites irréductibles provient du lemme suivant :

Lemme 5.3. $\Pr[C_r] \leq \sum_{\alpha \in \mathcal{I}_{r-1}} \Pr[B_{r,\alpha}]$. ▽

Démonstration. Montrons par récurrence sur r que $C_r \subseteq \cup_{\alpha \in \mathcal{I}_{r-1}} B_{r,\alpha}$, ce qui prouvera le lemme. On commence par le montrer directement pour $r = 2, 3, 4$. C'est trivial pour $r = 2$ puisque $C_2 = A_1 \cup A_2 = B_{2,0} \cup B_{2,1}$ et les deux suites 0 et 1 sont irréductibles. Pour $r = 3$, on a :

$$C_3 = (A_1 \cup A_2)(A_2 \cup A_3) \subseteq A_1 A_3 \cup A_2 = B_{3,01} \cup B_{3,10}\,,$$

et 01 et 10 sont irréductibles tandis que 00 et 11 sont réductibles. Pour $r = 4$, on a :

$$\begin{aligned} C_4 = (A_1 \cup A_2)(A_2 \cup A_3)(A_3 \cup A_4) &\subseteq A_1 A_3 \cup A_2 A_3 \cup A_2 A_4 \\ &\subseteq B_{4,010} \cup B_{4,100} \cup B_{4,101}\,, \end{aligned}$$

et 010, 100, et 101 sont les seules suites irréductibles de longueur 3.

Montrons maintenant que le lemme reste vrai pour $r \geq 5$. Supposons qu'il est vrai pour $r - 1$, alors :

$$\begin{aligned} C_r = C_{r-1} \cap (A_{r-1} \cup A_r) &\subseteq \left(\cup_{\alpha \in \mathcal{I}_{r-2}} B_{r-1,\alpha}\right) \cap (A_{r-1} \cup A_r) \\ &\subseteq \left(\cup_{\alpha \in \mathcal{I}_{r-2}} B_{r-1,\alpha} A_{r-1}\right) \cup \left(\cup_{\alpha \in \mathcal{I}_{r-2}} B_{r-1,\alpha} A_r\right) \\ &\subseteq \left(\cup_{\alpha \in \mathcal{I}_{r-2}} B_{r,\alpha 0}\right) \cup \left(\cup_{\alpha \in \mathcal{I}_{r-2}} B_{r,\alpha 1}\right) \end{aligned}$$

Ainsi, il suffit de montrer que, pour toute suite irréductible $\alpha \in \mathcal{I}_{r-2}$ telle que $\alpha 0$, respectivement $\alpha 1$, est réductible, il existe une suite irréductible $\bar{\alpha} \in \mathcal{I}_{r-1}$ telle que $B_{r,\alpha 0} \subseteq B_{r,\bar{\alpha}}$, respectivement $B_{r,\alpha 1} \subseteq B_{r,\bar{\alpha}}$. On distingue trois cas possibles en fonction de la forme de $\alpha \in \mathcal{I}_{r-2}$. Remarquons que, puisqu'on a supposé que $r - 2 \geq 3$, α contient au moins un motif 10 ou un motif 100, de telle façon que soit $\alpha = \alpha' 10$, soit $\alpha = \alpha' 100$, soit $\alpha = \alpha' 1$, avec $\alpha' \in \{\lambda, 0\}\{10, 100\}^*$ dans chaque cas.

- Cas 1 : $\alpha = \alpha' 10$; dans ce cas, on voit que $\alpha 0 = \alpha' 100$ et $\alpha 1 = \alpha' 101$ sont irréductibles.
- Cas 2 : $\alpha = \alpha' 100$; dans ce cas, $\alpha 1 = \alpha' 1001$ est irréductible mais $\alpha 0 = \alpha' 1000$ est réductible. Soit $\bar{\alpha} = \alpha' 1010$. Remarquons que $\bar{\alpha}$ est irréductible. De plus :

  $$\begin{aligned} B_{r,\alpha 0} = B_{r,\alpha' 1000} &= B_{r-4,\alpha'} \cap A_{r-3} A_{r-2} A_{r-1} \\ B_{r,\bar{\alpha}} = B_{r,\alpha' 1010} &= B_{r-4,\alpha'} \cap A_{r-3} A_{r-1}\,, \end{aligned}$$

  et donc $B_{r,\alpha 0} \subseteq B_{r,\bar{\alpha}}$.
- Cas 3 : $\alpha = \alpha' 1$; dans ce cas, $\alpha 0 = \alpha' 10$ est irréductible mais $\alpha 1 = \alpha' 11$ est réductible. Soit $\bar{\alpha} = \alpha' 10$. Remarquons que $\bar{\alpha}$ est irréductible. De plus :

  $$\begin{aligned} B_{r,\alpha 1} = B_{r,\alpha' 11} &= B_{r-2,\alpha'} \cap A_{r-1} A_r \\ B_{r,\bar{\alpha}} = B_{r,\alpha' 10} &= B_{r-2,\alpha'} \cap A_{r-1}\,, \end{aligned}$$

  et donc $B_{r,\alpha 1} \subseteq B_{r,\bar{\alpha}}$.

Ainsi $C_r \subseteq \cup_{\alpha \in \mathcal{I}_{r-1}} B_{r,\alpha}$, ce qui prouve le lemme. ∎

On donne maintenant une majoration des probabilités des événements $B_{r,\alpha}$ pour les suites irréductibles α. Pour cela, on introduit la définition suivante :

Définition 5.3
Le poids d'une suite $\alpha \in \{0,1\}^*$, noté $\mathbf{w}(\alpha)$, est le nombre de motifs 10 qu'elle contient (c'est-à-dire le nombre d'entiers i tels que $\alpha_i = 1$ et $\alpha_{i+1} = 0$). ♦

Lemme 5.4. *Soit $\alpha \in \{0,1\}^{r-1}$ une suite irréductible. Alors :*

$$\Pr[B_{r,\alpha}] \leq p^{r-1-\mathbf{w}(\alpha)}\,. \qquad \triangledown$$

Démonstration. Soit $k = \mathbf{w}(\alpha)$. Par définition, il y a exactement k entiers distincts $i_1 < \ldots < i_k$ tels que, pour chaque $i \in \{i_1, \ldots, i_k\}$, on a $\alpha_i = 1$ et $\alpha_{i+1} = 0$, ce qui implique que $A_{i+\alpha_i} A_{i+1+\alpha_{i+1}} = A_{i+1} = A_{i+\alpha_i}$. Ainsi, on voit que :

$$B_{r,\alpha} \subseteq \bigcap_{\substack{i=1 \\ i \neq i_1+1,\ldots,i_k+1}}^{r-1} A_{i+\alpha_i}\,.$$

Le lemme 5.1 et le fait que l'événement dans la partie droite est l'intersection de $r-1-k$ événements distincts A_j permettent de conclure. ∎

Il reste à compter le nombre de suites irréductibles d'un poids donné.

Lemme 5.5. *Le nombre de suites irréductibles de longueur r et de poids k est égal à $\binom{k+2}{r-2k}$. De plus, le poids minimal et le poids maximal d'une suite irréductible sont respectivement $k_{\min} = \lceil \frac{r-2}{3} \rceil$ et $k_{\max} = \lfloor \frac{r}{2} \rfloor$.* $\triangledown$

Démonstration. Soient a et b le nombre de motifs 10 et 100 dans une suite irréductible donnée. Clairement, le poids k de la suite vérifie $k = a + b$. De plus, en fonction de si la suite commence par un 0 et se termine par un 1, on a la relation suivante entre a, b et la longueur r de la suite :

- pour les suites de la forme $\lambda\{10,100\}^*\lambda$, on a $2a + 3b = r$
- pour les suites de la forme $0\{10,100\}^*\lambda$ ou $\lambda\{10,100\}^*1$, on a $2a + 3b = r - 1$
- pour les suites de la forme $0\{10,100\}^*1$, on a $2a + 3b = r - 2$

En notant $r' = r$, $r-1$ ou $r-2$ en fonction des cas, on a toujours $2a + 3b = r'$, ce qui, combiné avec $a+b = k$, implique $b = r' - 2k$. Pour chaque cas, le nombre de suites possibles est égal à $\binom{a+b}{b} = \binom{k}{r'-2k}$. Ainsi, le nombre total de suites irréductibles de longueur r et de poids k est :

$$\binom{k}{r-2k} + 2\binom{k}{r-1-2k} + \binom{k}{r-2-2k} = \binom{k+2}{r-2k}\,.$$

Le poids minimal et le poids maximal d'une suite irréductible s'obtiennent en observant les valeurs extrémales, non nulles, de $\binom{k+2}{r-2k}$ pour k vérifiant $0 \leq r - 2k \leq k + 2$. ∎

Nous sommes maintenant prêts pour prouver le résultat principal de cette section, c'est-à-dire majorer $\Pr[C_r]$ de la façon suivante :

TABLE 5.1 – Forme développée et réduite de C_r et majoration de $\Pr[C_r]$ pour r de 2 à 8.

r	C_r (développé et réduit)	majoration de $\Pr[C_r]$
2	$A_1 \cup A_2$	$2p$
3	$A_1A_3 \cup A_2$	$p + p^2$
4	$A_1A_3 \cup A_2A_3 \cup A_2A_4$	$3p^2$
5	$A_1A_3A_4 \cup A_1A_3A_5 \cup A_2A_3A_5 \cup A_2A_4$	$p^2 + 3p^3$
6	$A_1A_3A_4A_6 \cup A_1A_3A_5 \cup A_2A_3A_5 \cup A_2A_4A_5 \cup A_2A_4A_6$	$4p^3 + p^4$
7	$A_1A_3A_4A_6 \cup A_1A_3A_5A_6 \cup A_1A_3A_5A_7 \cup A_2A_3A_5A_6 \cup$ $A_2A_3A_5A_7 \cup A_2A_4A_5A_7 \cup A_2A_4A_6$	$p^3 + 6p^4$
8	$A_1A_3A_4A_6A_7 \cup A_1A_3A_4A_6A_8 \cup A_1A_3A_5A_6A_8 \cup$ $A_1A_3A_5A_7 \cup A_2A_3A_5A_6A_8 \cup A_2A_3A_5A_7 \cup$ $A_2A_4A_5A_7 \cup A_2A_4A_6A_7 \cup A_2A_4A_6A_8$	$5p^4 + 4p^5$

Lemme 5.6. *Soit $A_1, \ldots, A_r$ une suite p-négativement dépendante. Alors :*

$$\Pr\left[\bigcap_{i=1}^{r-1}(A_i \cup A_{i+1})\right] \leq \sum_{k=\lfloor \frac{r}{2} \rfloor}^{\lfloor \frac{2r}{3} \rfloor} \binom{r+1-k}{2r-3k} p^k \,. \qquad \triangledown$$

DÉMONSTRATION. En combinant les lemmes 5.3, 5.4, et 5.5 (remarquons qu'on applique ce dernier lemme aux suites de longueur $r-1$), on a :

$$\Pr[C_r] \leq \sum_{k=\lceil \frac{r-3}{3} \rceil}^{\lfloor \frac{r-1}{2} \rfloor} \binom{k+2}{r-1-2k} p^{r-1-k} \,.$$

ce qui, après avoir effectué le changement de variable $r-1-k \leftarrow k'$, permet de conclure.■

Nous pouvons vérifier le lemme 5.6 en développant et réduisant C_r pour les premières valeurs de r (voir table 5.1 pour la majoration obtenue pour les valeurs de r de 2 à 8).

5.3 Indistinguabilité des schémas de Feistel à clés alternées face à une attaque NCPA

Dans cette section, nous allons prouver l'indistinguabilité des schémas de Feistel à clés alternées en utilisant la stratégie de preuve par coupling habituelle.

Bien qu'un KAF soit, en quelque sorte, un schéma d'Even-Mansour itéré, les preuves de sécurité pour le schéma d'Even-Mansour itéré ne se transposent pas au KAF. En particulier, bien qu'un schéma d'Even-Mansour itéré sur $2n$ bits soit sûr jusqu'à $\mathcal{O}(2^n)$ requêtes, un KAF à 2 tours est facilement distinguable d'une permutation uniformément aléatoire en utilisant seulement deux requêtes directes : on envoie les requêtes (x_L, x_R) et (x'_L, x_R), et on vérifie si les chiffrés respectifs (y_L, y_R) et (y'_L, y'_R) vérifient $y_L \oplus y'_L = x_L \oplus x'_L$).

5.3.1 Distingueurs NCPA et CCA

Afin d'étudier l'indistinguabilité d'un KAF, nous considérons un distingueur $\mathcal{D}$ interagissant avec r oracles de fonctions $\boldsymbol{F} = (F_0, \ldots, F_{r-1})$ de $\mathcal{F}_n$ et un oracle de permutation de $\mathcal{P}_{2n}$ (et potentiellement son inverse pour le cas d'un distingueur CCA) qui se comporte soit comme le KAF $\mathtt{KAF}_k^{\boldsymbol{F}}$ avec une clé uniformément aléatoire $k = (k_0, \ldots, k_{r-1})$, soit comme une permutation aléatoire uniforme P (indépendante de $\boldsymbol{F}$). Un (q_e, q_f)-distingueur est un distingueur qui fait au plus q_e requêtes à l'oracle de permutation et au plus q_f requêtes à chaque fonction de tours $F_0, \ldots, F_{r-1}$. Comme d'habitude, on ne considère que les attaquants ayant une capacité de calculs non borné et on se restreint, sans perte de généralité, à des attaquants déterministes qui ne font jamais de requêtes redondantes et font toujours le nombre maximal autorisé de requêtes.

Comme nous l'avons fait pour le schéma d'Even-Mansour itéré, on définit deux types de distingueurs : les distingueurs NCPA et les distingueurs CCA. Le caractère NCPA ou CCA s'applique à la façon d'agir avec l'oracle de permutation mais, dans les deux cas, les requêtes aux fonctions internes peuvent se faire de manière adaptative. Plus précisément :

Définition 5.4 (Distingueur NCPA et CCA)
Un $(q_e, q_f)-$distingueur NCPA $\mathcal{D}$ agit en deux étapes :

1. Dans un premier temps, le distingueur $\mathcal{D}$ fait exactement q_f requêtes à chaque fonction interne F_i. Ces requêtes peuvent être adaptatives.
2. Dans un second temps, le distingueur $\mathcal{D}$ choisit un q_e-uplet de requêtes $(x^1, \ldots, x^{q_e})$, de manière non-adaptative, qu'il envoie à l'oracle de permutation et reçoit les réponses $(y^1, \ldots, y^{q_e})$. Ces requêtes sont donc directes et non-adaptatives, elles peuvent en revanche dépendre des réponses obtenues pendant la première étape.

   Un $(q_e, q_f)-$distingueur CCA est le plus général : il fait q_f requêtes à chaque F_i et q_e requêtes à l'oracle de permutation. Toutes ses requêtes sont adaptatives et dans l'ordre qu'il souhaite (il peut alterner les requêtes à l'oracle de permutation et aux fonctions de tours). ♦

5.3.2 Notations

La probabilité d'un événement E quand $\mathcal{D}$ interagit avec $(\boldsymbol{F}, P)$, où P est une permutation uniformément aléatoire et indépendante des fonctions de tours $\boldsymbol{F}$, sera notée $\Pr^*[E]$, tandis que la probabilité d'un événement E quand $\mathcal{D}$ interagit avec $(\boldsymbol{F}, \mathtt{KAF}_k^{\boldsymbol{F}})$, où $k = (k_0, \ldots, k_{r-1})$ est uniformément aléatoire, sera notée $\Pr[E]$. Avec ces notations, l'avantage d'un distingueur $\mathcal{D}$ est défini comme $|\Pr[\mathcal{D}(1^n) = 1] - \Pr^*[\mathcal{D}(1^n) = 1]|$ (nous omettons les oracles dans la notation car ils se déduisent des notations $\Pr[\cdot]$ et $\Pr^*[\cdot]$). L'avantage maximal d'un (q_e, q_f)-distingueur ATK (où ATK est NCPA ou CCA) contre un KAF à r tours avec des fonctions de tours dans $\mathcal{F}_n$ sera noté $\mathbf{Adv}^{\mathrm{atk}}_{\mathtt{KAF}[n,r]}(q_e, q_f)$.

Quand $q_f = 0$, c'est-à-dire quand le distingueur ne peut pas faire de requêtes aux fonctions de tours, il n'est pas difficile de voir que les clés $k_0, \ldots, k_{r-1}$ ne contribuent pas à la sécurité du schéma et on peut donc les fixer à zéro. Ainsi, on retrouve le cadre de Luby-Rackoff où les fonctions de tours sont uniformément aléatoires et jouent le rôle de clés secrètes (ainsi, l'espace des clés est $(\mathcal{F}_n)^r$). Dans ce cadre, nos définitions d'un distingueur NCPA et d'un distingueur CCA correspondent aux définitions habituelles pour un schéma de chiffrement par blocs dans le modèle standard (c'est-à-dire quand il n'y a pas d'oracles

additionnels). Nous noterons $\mathbf{Adv}^{\mathrm{atk}}_{\mathtt{LR}[n,r]}(q_e)$ l'avantage d'un $(q_e, q_f = 0)$-distingueur ATK contre le schéma de Luby-Rackoff classique à r tours.

Pour résumer, on considère un cadre unique pour étudier deux types de schémas de Feistel : les schémas de Feistel classiques à la Luby-Rackoff où les fonctions de tours sont aléatoires et secrètes, et les KAF où les fonctions de tours sont de la forme $F_i(x \oplus k_i)$, où les k_i sont des clés de tours secrètes et les F_i des oracles publiques implémentant des fonctions uniformément aléatoires.

5.3.3 Lien entre avantage et distance statistique (étape 1)

Comme d'habitude, nous commençons par établir le lien entre avantage et distance statistique. On s'intéresse à l'avantage d'un distingueur NCPA pour distinguer un KAF à r tours $\mathtt{KAF}[n,r]$ d'une permutation aléatoire. Pour cela, nous allons majorer la distance statistique entre les sorties du KAF, conditionné par des informations partielles sur les fonctions de tours F_i, et la distribution uniforme sur $(\mathcal{I}_{2n})^{*q_e}$.

Pour tout uplet $u = (u_0, \ldots, u_{r-1})$ et $v = (v_0, \ldots, v_{r-1})$ avec $u_i = (u_i^1, \ldots, u_i^{q_f}), v_i = (v_i^1, \ldots, v_i^{q_f}) \in (\{0,1\}^n)^{q_f}$, et $x \in (\mathcal{I}_{2n})^{*q_e}$, on note $\mu_{x,u,v}$ la distribution du q_e-uplet $y = \mathtt{KAF}_k^{\boldsymbol{F}}(x)$ où la clé $k = (k_0, \ldots, k_{r-1})$ est uniformément aléatoires, et les fonctions de tours $\boldsymbol{F} = (F_0, \ldots, F_{r-1})$ sont uniformément aléatoire parmi les fonctions vérifiant$\boldsymbol{F}(u) = v$ (c'est-à-dire $F_i(u_i^j) = v_i^j$ pour tout $i \leq r-1$ et $j \leq q_f$). Dans le cadre de Luby-Rackoff ($q_f = 0$), nous noterons simplement μ_x. On note également μ^* la distribution uniforme sur $(\mathcal{I}_{2n})^{*q_e}$. On peut alors énoncer le lemme suivant :

Lemme 5.7. *Soit q_e, q_f des entiers positifs. Supposons qu'il existe α tel que, pour tout uplet $u = (u_0, \ldots, u_{r-1})$, $v = (v_0, \ldots, v_{r-1})$ avec $u_i, v_i \in (\{0,1\}^n)^{q_f}$, et $x \in (\mathcal{I}_{2n})^{*q_e}$, on a $\|\mu_{x,u,v} - \mu^*\| \leq \alpha$. Alors $\mathbf{Adv}^{\mathrm{ncpa}}_{\mathtt{KAF}[n,r]}(q_e, q_f) \leq \alpha$.* ▽

Démonstration. La preuve est similaire au lemme 3.2 du chapitre 3.

5.3.4 Diviser pour mieux régner (étape 2)

Dans cette section, nous allons diviser le problème de la majoration de $\|\mu_{x,u,v} - \mu^*\|$ en q_e problèmes de majoration plus simple. Fixons des uplets $u = (u_0, \ldots, u_{r-1})$, $v = (v_0, \ldots, v_{r-1})$ avec $u_i = (u_i^1, \ldots, u_i^{q_f}) \in (\{0,1\}^n)^{q_f}$ et $v_i = (v_i^1, \ldots, v_i^{q_f}) \in (\{0,1\}^n)^{q_f}$, et $x = (x^1, \ldots, x^{q_e}) \in (\mathcal{I}_{2n})^{*q_e}$.

Pour $0 \leq \ell \leq q_e - 1$, on note ν_ℓ la distribution des $(\ell+1)$ sorties du KAF quand il reçoit les entrées $(x^1, \ldots, x^\ell, x^{\ell+1})$, et ν_ℓ^* la distribution des $(\ell+1)$ sorties du KAF quand il reçoit les entrées $(x^1, \ldots, x^\ell, z^{\ell+1})$, où $z^{\ell+1}$ est uniformément distribué sur $\{0,1\}^{2n} \setminus \{x^1, \ldots, x^\ell\}$ (dans les deux cas, la clé $k = (k_0, \ldots, k_{r-1})$ est uniformément aléatoire, et les fonctions de tours $\boldsymbol{F} = (F_0, \ldots, F_{r-1})$ sont uniformément aléatoires parmi les fonctions vérifiant $\boldsymbol{F}(u) = v$). Alors, on obtient le lemme suivant dont la preuve est similaire à celle du [MRS09, Lemme 2] (ce lemme n'est pas spécifique à notre schéma et s'applique à tout schéma de chiffrement par blocs).

Lemme 5.8. $\|\mu_{x,u,v} - \mu^*\| \leq \sum_{\ell=0}^{q_e-1} \|\nu_\ell - \nu_\ell^*\|$. ▽

Démonstration. On rappelle que, pour toute distribution μ et ν sur le même ensemble Ω, il existe toujours un coupling λ_{op} de μ et ν, appelé coupling *optimal*, vérifiant :

$$\|\mu - \nu\| = \Pr_{(X,Y)\sim\lambda_{\text{op}}}[X \neq Y]\,.$$

Pour toute distribution ν sur les q_e-uplets d'éléments distincts de $\{0,1\}^{2n}$, et pour tout $(y^1,\ldots,y^\ell) \in (\mathcal{I}_{2n})^{*\ell}$ avec $\ell \geq 0$, on note

$$\nu(y^{\ell+1}|y^1,\ldots,y^\ell) = \Pr[Y^{\ell+1} = y^{\ell+1}|Y^1 = y^1,\ldots,Y^\ell = y^\ell]\,,$$

où $(Y^1,\ldots,Y^{q_e}) \sim \nu$. Pour $\ell = 0$, on note simplement $\nu(\cdot|\Omega)$ la distribution (non conditionnée) de la première coordonnée Y^1 (Ω correspond à l'univers entier).

On définit le coupling de (Y,Z), où $Y = (Y^1,\ldots,Y^{q_e}) \sim \mu_{x,u,v}$ et $Z = (Z^1,\ldots,Z^{q_e}) \sim \mu^*$, comme suit. Tout d'abord, on tire (Y_1,Z_1) selon le coupling optimal de $\mu_{x,u,v}(\cdot|\Omega)$ et $\mu^*(\cdot|\Omega)$. Puis, pour $\ell = 1\ldots,q_e-1$: si $(Y^1,\ldots,Y^\ell) = (Z^1,\ldots,Z^\ell) = (y^1,\ldots,y^\ell)$, on tire $(Y^{\ell+1},Z^{\ell+1})$ selon le coupling optimal de $\mu_{x,u,v}(\cdot|y^1,\ldots,y^\ell)$ et $\mu^*(\cdot|y^1,\ldots,y^\ell)$. Sinon, si $(Y^1,\ldots,Y^\ell) \neq (Z^1,\ldots,Z^\ell)$, on couple $(Y^{\ell+1},Z^{\ell+1})$ de manière arbitraire.

Alors, par le lemme du coupling, on a :

$$\begin{aligned}
\|\mu_{x,u,v} - \mu^*\| &\leq \Pr[Y \neq Z] \\
&\leq \sum_{\ell=0}^{q_e-1} \Pr[(Y^1,\ldots,Y^\ell) = (Z^1,\ldots,Z^\ell) \wedge Y^{\ell+1} \neq Z^{\ell+1}] \\
&\leq \sum_{\ell=0}^{q_e-1} \sum_{(y^1,\ldots,y^\ell)} \Pr_{Y\sim\mu_{x,u,v}}[(Y^1,\ldots,Y^\ell) = (y^1,\ldots,y^\ell)]\times \\
&\qquad \Pr[Y^{\ell+1} \neq Z^{\ell+1}|(Z^1,\ldots,Z^\ell) = (Y^1,\ldots,Y^\ell) = (y^1,\ldots,y^\ell)] \\
&\leq \sum_{\ell=0}^{q_e-1} \sum_{(y^1,\ldots,y^\ell)} \Pr_{Y\sim\mu_{x,u,v}}[(Y^1,\ldots,Y^\ell) = (y^1,\ldots,y^\ell)]\times \\
&\qquad \|\mu_{x,u,v}(\cdot|y^1,\ldots,y^\ell) - \mu^*(\cdot|y^1,\ldots,y^\ell)\| \\
&\leq \sum_{\ell=1}^{q_e-1} \mathbb{E}_{Y\sim\mu_{x,u,v}}\left[\|\mu_{x,u,v}(\cdot|Y^1,\ldots,Y^\ell) - \mu^*(\cdot|Y^1,\ldots,Y^\ell)\|\right]\,,
\end{aligned}$$

où

$$\begin{aligned}
\mathbb{E}_{Y\sim\mu_{x,u,v}}\left[\|\mu_{x,u,v}(\cdot|Y^1,\ldots,Y^\ell) - \mu^*(\cdot|Y^1,\ldots,Y^\ell)\|\right] = \\
\sum_{(y^1,\ldots,y^\ell)} \Pr_{Y\sim\mu_{x,u,v}}[(Y^1,\ldots,Y^\ell) = (y^1,\ldots,y^\ell)]\times \\
\|\mu_{x,u,v}(\cdot|y^1,\ldots,y^\ell) - \mu^*(\cdot|y^1,\ldots,y^\ell)\|\,.
\end{aligned}$$

L'avant dernière inégalité provient du fait que, lorsque $(Y^1,\ldots,Y^\ell) = (Z^1,\ldots,Z^\ell) = (y^1,\ldots,y^\ell)$, $(Y^{\ell+1},Z^{\ell+1})$ est choisie selon le coupling optimal de $\mu_{x,u,v}(\cdot|y^1,\ldots,y^\ell)$ et $\mu^*(\cdot|y^1,\ldots,y^\ell)$.

On sait également que :

$$\begin{aligned}
\|\nu_\ell - \nu_\ell^*\| &= \frac{1}{2} \sum_{(y^1,\ldots,y^{\ell+1})} |\nu_\ell(y^1,\ldots,y^{\ell+1}) - \nu_\ell^*(y^1,\ldots,y^{\ell+1})| \\
&= \frac{1}{2} \sum_{(y^1,\ldots,y^{\ell+1})} \nu_{\ell-1}(y^1,\ldots,y^\ell)\times \\
&\qquad\qquad |\mu_{x,u,v}(y^{\ell+1}|y^1,\ldots,y^\ell) - \mu^*(y^{\ell+1}|y^1,\ldots,y^\ell)| \\
&= \sum_{(y^1,\ldots,y^\ell)} \nu_{\ell-1}(y^1,\ldots,y^\ell)\|\mu_{x,u,v}(\cdot|y^1,\ldots,y^\ell) - \mu^*(\cdot|y^1,\ldots,y^\ell)\| \\
&= \mathbb{E}_{Y\sim\mu_{x,u,v}}\left[\|\mu_{x,u,v}(\cdot|Y^1,\ldots,Y^\ell) - \mu^*(\cdot|Y^1,\ldots,Y^\ell)\|\right],
\end{aligned}$$

ce qui permet de conclure.

5.3.5 Coupler les deux distributions adjacentes (étape 3)

On s'intéresse maintenant à majorer $\|\nu_\ell - \nu_\ell^*\|$ pour $0 \le \ell \le q_e - 1$. Notre objectif est de définir un coupling de ν_ℓ et ν_ℓ^*, c'est-à-dire une distribution jointe sur les paires d'uplets de $\ell+1$ chaînes de $2n$ bits, dont les distributions marginales sont ν_ℓ et ν_ℓ^*. Pour cela, on considère parallèlement deux KAF. Le premier, $\texttt{KAF}_k^{\boldsymbol{F}}$, prend comme entrées $(x^1,\ldots,x^\ell,x^{\ell+1})$, tandis que le second, $\texttt{KAF}_{k'}^{\boldsymbol{F}'}$, où $\boldsymbol{F}' = (F'_0,\ldots,F'_{r-1})$, prend comme entrées $(x^1,\ldots,x^\ell,z^{\ell+1})$, où $z_{\ell+1}$ est n'importe quelle valeur dans $\{0,1\}^{2n}\setminus\{x^1,\ldots,x^\ell\}$ (on majore la distance statistique entre les sorties des deux systèmes pour tout $z_{\ell+1}$, ainsi, la même borne supérieure reste valide quand $z^{\ell+1}$ est choisie uniformément aléatoire dans $\{0,1\}^{2n}\setminus\{x^1,\ldots,x^\ell\}$). On choisit k uniformément aléatoire et $\boldsymbol{F}$ uniformément aléatoire parmi les fonctions vérifiant $\boldsymbol{F}(u) = v$. Nous allons définir k' et $\boldsymbol{F}'$ de sorte qu'ils vérifient les mêmes propriétés. Cela assurera que les distribution marginales des sorties du premier KAF et du second KAF sont bien, respectivement, ν_ℓ et ν_ℓ^*.

Le coupling

Nous présentons maintenant de quelle manière le coupling est défini. Tout d'abord, les clés de tours du second KAF sont choisies égales aux clés de tours du premier KAF, c'est-à-dire $k' = k$. Pour $1 \le j \le \ell+1$, soient x_{-1}^j et x_0^j les deux moitiés de n bits, respectivement, gauche et droite de x^j et, pour $1 \le i \le r$, soit x_i^j défini récursivement par $x_i^j = x_{i-2}^j \oplus F_{i-1}(x_{i-1}^j \oplus k_{i-1})$ (voir figure 5.2). Pour tout $1 \le j \le \ell$ et tout $0 \le i \le r-1$, on fixe F' tel que $F'_i(x_i^j \oplus k_i) = F_i(x_i^j \oplus k_i)$ (notons que cela est compatible avec la condition $\boldsymbol{F}'(u) = v$ au cas où une valeur $x_i^j \oplus k_i$ appartient à $u_i = (u_i^1,\ldots,u_i^{q_f})$, l'ensemble des requêtes du distingueur à la fonction de tours F_i). Puisque les ℓ premières requêtes au deuxième KAF sont les mêmes que celles du premier KAF, cela assure que les ℓ premières sorties des deux KAF sont égales. Il reste à définir le coupling pour la requête $(\ell+1)$. Soient $z_{-1}^{\ell+1}$ et $z_0^{\ell+1}$ les deux moitiés de n bits, respectivement, gauche et droite de $z^{\ell+1}$. On définit récursivement, pour $1 \le i \le r$, les valeurs $z_i^{\ell+1} = z_{i-2}^{\ell+1} \oplus F'_{i-1}(z_{i-1}^{\ell+1} \oplus k_{i-1})$. Pour cela, on définit deux événements « bad » qui peuvent se produire aux tours $0 \le i \le r-1$ dans chacun des KAF. On définit $\texttt{XColl}_i$ l'événement « $x_i^{\ell+1} \oplus k_i$ est égal à $x_i^j \oplus k_i$ pour un certain $1 \le j \le \ell$ » (c'est-à-dire que la valeur d'entrée de F_i quand on chiffre $x^{\ell+1}$ collisionne avec la valeur d'entrée de F_i quand on chiffre une requête précédente x^j). On définit $\texttt{FColl}_i$

l'événement « $x_i^{\ell+1} \oplus k_i \in u_i$ » (c'est-à-dire que la valeur d'entrée de F_i quand on chiffre $x^{\ell+1}$ est égale à l'une des requêtes faites à F_i par le distingueur). On note simplement $\texttt{Coll}_i = \texttt{XColl}_i \cup \texttt{FColl}_i$. De la même manière, on définit $\texttt{XColl}'_i$ l'événement « $z_i^{\ell+1} \oplus k_i$ est égal à un certain $x_i^j \oplus k_i$ pour $1 \le j \le \ell$ », $\texttt{FColl}'_i$ l'événement « $z_i^{\ell+1} \oplus k_i \in u_i$ », et on note $\texttt{Coll}'_i = \texttt{XColl}'_i \cup \texttt{FColl}'_i$. Alors, pour $i = 0, \ldots, r-1$, on définit $F'_i(z_i^{\ell+1} \oplus k_i)$ par :

(1) si $\texttt{Coll}'_i$ est vrai, alors $F'_i(z_i^{\ell+1} \oplus k_i)$ est déjà défini (soit car $z_i^{\ell+1} \oplus k_i = x_i^j \oplus k_i$ pour un certain $j \le \ell$, soit par la contrainte $\boldsymbol{F}'(u) = v$) ;

(2) si $\texttt{Coll}'_i$ est faux mais $\texttt{Coll}_i$ est vrai, $F'_i(z_i^{\ell+1} \oplus k_i)$ est choisi uniformément aléatoire ;

(3) si $\texttt{Coll}_i$ et $\texttt{Coll}'_i$ sont faux, alors on définit $F'_i(z_i^{\ell+1} \oplus k_i)$ de telle façon que $z_{i+1}^{\ell+1} = x_{i+1}^{\ell+1}$, c'est-à-dire :

$$F'_i(z_i^{\ell+1} \oplus k_i) = z_{i-1}^{\ell+1} \oplus x_{i-1}^{\ell+1} \oplus F_i(x_i^{\ell+1} \oplus k_i)\,.$$

Vérification que les distributions marginales sont respectées

On peut vérifier que les fonctions de tours $\boldsymbol{F}'$, dans le second KAF, sont uniformément aléatoires parmi les uplets de fonctions vérifiant $\boldsymbol{F}'(u) = v$. C'est clair quand $F'_i(z_i^{\ell+1} \oplus k_i)$ est défini par les règles (1) ou (2). Quand $F'_i(z_i^{\ell+1} \oplus k_i)$ est défini par la règle (3), alors $F_i(x_i^{\ell+1} \oplus k_i)$ est uniformément aléatoire puisque $\texttt{Coll}_i$ est faux et donc $F'_i(z_i^{\ell+1} \oplus k_i)$ est également uniformément aléatoire. Lorsque $z_{\ell+1}$ est choisi uniformément aléatoire, cela implique que les sorties du second KAF sont distribuées selon ν_ℓ^* comme prévu.

On dit que le coupling est réussi si toutes les sorties du second KAF sont égales aux sorties du premier KAF. Puisque les ℓ premières sorties sont égales entre les deux KAFs (par construction), le coupling est réussi si et seulement si $z_{r-1}^{\ell+1} = x_{r-1}^{\ell+1}$ et $z_r^{\ell+1} = x_r^{\ell+1}$.

Probabilité que le coupling échoue

Le lemme suivant établit l'une des idées clés du coupling : si les états, juste après un tour i, en chiffrant $x^{\ell+1}$ dans le premier KAF et en chiffrant $z^{\ell+1}$ dans le second KAF, sont égaux, alors ils le restent dans les tours qui suivent :

Lemme 5.9. *Si il existe $i \le r-1$ tel que $z_i^{\ell+1} = x_i^{\ell+1}$ et $z_{i+1}^{\ell+1} = x_{i+1}^{\ell+1}$, alors le coupling est réussi.* ▽

Démonstration. On procède par récurrence. Si $i = r-1$, il n'y a rien à prouver. Fixons $i < r-1$, et supposons que la propriété est vérifiée pour $i+1$. Alors, si $z_i^{\ell+1} = x_i^{\ell+1}$ et $z_{i+1}^{\ell+1} = x_{i+1}^{\ell+1}$, on doit simplement prouver que $z_{i+2}^{\ell+1} = x_{i+2}^{\ell+1}$ et le coupling sera réussi à l'aide de l'hypothèse de récurrence.

Si $\texttt{Coll}'_{i+1}$ est vrai, c'est-à-dire $z_{i+1}^{\ell+1} \oplus k_{i+1}$ est égal à $x_{i+1}^j \oplus k_{i+1}$ pour un certain $1 \le j \le \ell$ ou $u_{i+1}^{j'}$ pour un certain $1 \le j' \le q_f$, alors, dans les deux cas, on voit que $F'_{i+1}(z_{i+1}^{\ell+1} \oplus k_{i+1}) = F_{i+1}(x_{i+1}^{\ell+1} \oplus k_{i+1})$, de telle façon que :

$$z_{i+2}^{\ell+1} = z_i^{\ell+1} \oplus F'_{i+1}(z_{i+1}^{\ell+1} \oplus k_{i+1}) = x_i^{\ell+1} \oplus F_{i+1}(x_{i+1}^{\ell+1} \oplus k_{i+1}) = x_{i+2}^{\ell+1}\,.$$

Si $\texttt{Coll}'_{i+1}$ est faux, alors $\texttt{Coll}_{i+1}$ est également faux puisque on a supposé que $x_{i+1}^{\ell+1} = z_{i+1}^{\ell+1}$. Alors, par définition du coupling, $F'_{i+1}(z_{i+1}^{l+1} \oplus k_{i+1})$ est choisi tel que $z_{i+2}^{\ell+1} = x_{i+2}^{\ell+1}$. ■

Le lemme suivant établit que, si $\texttt{Coll}_i$ et $\texttt{Coll}'_i$ sont faux pour deux tours consécutifs, alors le coupling est réussi. Notons que, en général, on ne peut pas choisir le tour 0 pour

essayer de coupler car on ne peut empêcher le distingueur de choisir $x^{\ell+1}$ tel que $x_0^{\ell+1} = x_0^j$ pour un certain $j \leq \ell$, auquel cas $\texttt{Coll}_0$ est vrai avec probabilité 1.

Lemme 5.10. *Pour $i \in [1; r-1]$, on définit $A_i = \texttt{Coll}_i \cup \texttt{Coll}'_i$. Soit* `Fail` *l'événement « le coupling ne réussit pas », alors*

$$\Pr[\texttt{Fail}] \leq \Pr\left[\bigcap_{i=1}^{r-2}(A_i \cup A_{i+1})\right]. \qquad \triangledown$$

Démonstration. Fixons $i \in [1; r-2]$. Nous allons montrer que $\neg(A_i \cup A_{i+1}) \implies \neg\texttt{Fail}$. En effet, si $\texttt{Coll}_i$, $\texttt{Coll}'_i$, $\texttt{Coll}_{i+1}$, et $\texttt{Coll}'_{i+1}$ sont faux, alors, par définition du coupling, $F'_i(z_i^{\ell+1} \oplus k_i)$ et $F'_{i+1}(z_{i+1}^{\ell+1} \oplus k_{i+1})$ sont choisis tels que $z_{i+1}^{\ell+1} = x_{i+1}^{\ell+1}$ et $z_{i+2}^{\ell+1} = x_{i+2}^{\ell+1}$. Le lemme 5.9 implique alors que le coupling est réussi. On vient donc de prouver que $\neg\texttt{Fail} \supset \cup_{i=1}^{r-2}\neg(A_i \cup A_{i+1})$, ce qui prouve le lemme. ∎

Ainsi, la probabilité que le coupling échoue est exactement majorée par la probabilité de l'événement C_{r-1} que nous avons étudié à la section 5.2. A ce point, l'analyse diffère pour un KAF et pour un schéma de Luby-Rackoff. En effet, pour un schéma de Luby-Rackoff, on peut montrer que la suite d'événements A_i est p-négativement dépendante, ce qui n'est pas le cas pour un KAF.

5.3.6 Indistinguabilité d'un KAF face à une attaque NCPA (étapes 4 et 5)

Pour un KAF, on ne peut pas montrer que la suite d'événements A_i est p-négativement dépendante. Néanmoins, elle vérifie une forme plus faible de dépendance négative (remarquez que, dans le lemme suivant, $S \subseteq [1; i-2]$ et non $S \subseteq [1; i-1]$ si la suite A_i avait été p-négativement dépendante) :

Lemme 5.11. *Pour tout $i \in [1; r-1]$ et tout sous-ensemble $S \subseteq [1; i-2]$, on a :*

$$\Pr[A_i | \cap_{s\in S} A_s] \leq \frac{2(\ell + 2q_f)}{2^n}. \qquad \triangledown$$

Démonstration. Nous devons prouver que, pour tout $i \in [1; r-1]$ et tout sous-ensemble $S \subseteq [1; i-2]$, on a :

$$\Pr\left[\texttt{Coll}_i \cup \texttt{Coll}'_i \middle| \cap_{s\in S} A_s\right] \leq \frac{2(\ell + 2q_f)}{2^n}.$$

Nous majorons la probabilité conditionnelle de $\texttt{Coll}_i$, le raisonnement pour $\texttt{Coll}'_i$ est similaire. Rappelons que $\texttt{XColl}_i$ est l'événement « $x_i^{\ell+1} \oplus k_i$ est égal à $x_i^j \oplus k_i$ pour un certain $j \in [1; \ell]$ », et $\texttt{FColl}_i$ est l'événement « $x_i^{\ell+1} \oplus k_i$ est égal à $u_i^{j'}$ pour un certain $j' \in [1; q_f]$ », et $\texttt{Coll}_i = \texttt{XColl}_i \cup \texttt{FColl}_i$.

On commence par considérer la probabilité de $\texttt{FColl}_i$. Puisque k_i est uniformément aléatoire et indépendant de $\cap_{s\in S} A_s$, cette probabilité est au plus $q_f/2^n$.

On considère maintenant la probabilité de $\texttt{XColl}_i$, c'est-à-dire $x_i^{\ell+1} \oplus k_i = x_i^j \oplus k_i$ pour un certain $j \in [1; \ell]$. Remarquons que c'est équivalent à

$$x_{i-2}^{\ell+1} \oplus F_{i-1}(x_{i-1}^{\ell+1} \oplus k_{i-1}) = x_{i-2}^j \oplus F_{i-1}(x_{i-1}^j \oplus k_{i-1}). \qquad (5.1)$$

Ici, on fait face au problème que, conditionné sur $\texttt{FColl}_{i-1}$, $F_{i-1}(x_{i-1}^{\ell+1} \oplus k_{i-1})$ n'est plus uniformément aléatoire puisque $\boldsymbol{F}(u) = v$. Ainsi, en notant $B = \cap_{s\in S} A_s$, on peut écrire :

$$\begin{aligned}\Pr\left[\texttt{XColl}_i | B\right] &= \Pr\left[\texttt{XColl}_i | B \cap \texttt{FColl}_{i-1}\right] \Pr\left[\texttt{FColl}_{i-1} | B\right] \\ &\quad + \Pr\left[\texttt{XColl}_i | B \cap \overline{\texttt{FColl}_{i-1}}\right] \Pr\left[\overline{\texttt{FColl}_{i-1}} | B\right] \\ &\leq \Pr\left[\texttt{FColl}_{i-1} | B\right] + \Pr\left[\texttt{XColl}_i | B \cap \overline{\texttt{FColl}_{i-1}}\right] .\end{aligned}$$

Puisque k_{i-1} est uniformément aléatoire et indépendant de $B = \cap_{s\in S} A_s$ (on rappelle que $S \subseteq [1; i-2]$), on en déduit que $\Pr\left[\texttt{FColl}_{i-1} | B\right] \leq q_f/2^n$. Pour majorer la deuxième probabilité, remarquons que, si $x_{i-1}^{\ell+1} = x_{i-1}^{j}$, alors nécessairement $x_i^{\ell+1} \neq x_i^j$ puisque, sinon, cela contredirait l'hypothèse que les requêtes $x^{\ell+1}$ et x^j sont distinctes. Si $x_{i-1}^{\ell+1} \neq x_{i-1}^{j}$, alors, conditionné sur $\overline{\texttt{FColl}_{i-1}}$, $F_{i-1}(x_{i-1}^{\ell+1} \oplus k_{i-1})$ est uniformément aléatoire et l'équation (5.1) est vérifiée avec probabilité au plus 2^{-n} pour chaque j. Ainsi, en sommant sur les $j \in [1; \ell]$, on obtient que $\Pr\left[\texttt{XColl}_i | B \cap \overline{\texttt{FColl}_{i-1}}\right] \leq \ell/2^n$. Et donc $\Pr[\texttt{Coll}_i] \leq (\ell + 2q_f)/2^n$. Le raisonnement et les bornes sont similaires pour la probabilité de $\texttt{Coll}'_i$ ce qui permet de conclure. ∎

Lemme 5.12. *Soient q_e, q_f des entiers positifs. Alors, pour tout uplet $x \in (\mathcal{I}_{2n})^{*q_e}$ et $u = (u_0, \ldots, u_{r-1})$, $v = (v_0, \ldots, v_{r-1})$ avec $u_i, v_i \in (\{0,1\}^n)^{q_f}$, on a :*

$$\|\mu_{x,u,v} - \mu^*\| \leq \frac{4^t}{t+1} \frac{(q_e + 2q_f)^{t+1}}{2^{tn}} \quad \textit{avec} \quad t = \left\lfloor \frac{r}{3} \right\rfloor . \qquad \triangledown$$

Démonstration. En utilisant le lemme du coupling 2.1, le lemme 5.10 et le lemme 5.11, on a :

$$\begin{aligned}\|\nu_\ell - \nu_\ell^*\| \leq \Pr\left[\texttt{Fail}\right] &\leq \Pr\left[\bigcap_{i=1}^{r-2} (A_i \cup A_{i+1})\right] \\ &\leq \Pr\left[(A_1 \cup A_2)(A_4 \cup A_5) \cdots (A_{3\cdot\lfloor \frac{r}{3} \rfloor - 2} \cup A_{3\cdot\lfloor \frac{r}{3} \rfloor - 1})\right] \\ &\leq \left(\frac{4(\ell + 2q_f)}{2^n}\right)^t \quad \text{avec} \quad t = \left\lfloor \frac{r}{3} \right\rfloor .\end{aligned}$$

Ainsi, par le lemme 5.8, on déduit que, pour tous les uplets x, u, v :

$$\begin{aligned}\|\mu_{x,u,v} - \mu^*\| \leq \sum_{\ell=0}^{q_e-1} \|\nu_\ell - \nu_\ell^*\| &\leq \frac{4^t}{2^{tn}} \sum_{\ell=0}^{q_e-1} (\ell + 2q_f)^t \\ &\leq \frac{4^t}{2^{tn}} \int_{\ell=0}^{q_e} (\ell + 2q_f)^t \, d\ell \leq \frac{4^t}{t+1} \frac{(q_e + 2q_f)^{t+1}}{2^{tn}} ,\end{aligned}$$

ce qui permet de conclure.

Finalement, en combinant les lemmes 5.7 et 5.12, on obtient la borne de sécurité NCPA suivante pour un KAF :

Théorème 5.13. *Soient q_e, q_f des entiers positifs. Alors :*

$$\mathbf{Adv}^{\text{ncpa}}_{\texttt{KAF}[n,r]}(q_e, q_f) \leq \frac{4^t}{t+1} \frac{(q_e + 2q_f)^{t+1}}{2^{tn}} \quad \text{avec} \quad t = \left\lfloor \frac{r}{3} \right\rfloor . \qquad \diamondsuit$$

Ainsi, un KAF à r tours assure une sécurité NCPA jusqu'à $\mathcal{O}(N^{\frac{t}{t+1}})$ requêtes pour $t = \lfloor \frac{r}{3} \rfloor$.

5.3.7 Indistinguabilité du schéma de Luby-Rackoff face à une attaque NCPA (étapes 4 et 5)

Pour le schéma de Luby-Rackoff, les événements A_i sont p-négativement dépendants, ce que nous prouvons dans le lemme suivant. Cela va nous permettre d'utiliser les résultats de la section 5.2 pour majorer la probabilité que le coupling échoue et donc majorer l'avantage NCPA.

Lemme 5.14. *Dans le cadre d'un schéma de Luby-Rackoff ($q_f = 0$), les événements $A_1, \ldots, A_{r-1}$ sont p-négativement dépendants pour $p = \frac{2\ell}{2^n}$.* ▽

Démonstration. Nous devons prouver que, pour tout $i \in [1; r-1]$ et tout sous-ensemble $S \subseteq [1; i-1]$, on a :

$$\Pr\left[\texttt{Coll}_i \cup \texttt{Coll}'_i \middle| \cap_{s\in S} A_s\right] \leq \frac{2\ell}{2^n}\,.$$

Dans le cadre d'un schéma de Luby-Rackoff, $q_f = 0$ et donc $\texttt{FColl}_i$ et $\texttt{FColl}'_i$ sont toujours faux. Ainsi, on a simplement à étudier les événements $\texttt{XColl}_i$ et $\texttt{XColl}'_i$. L'événement $\texttt{XColl}_i$ est vrai si $x_i^{\ell+1} \oplus k_i = x_i^j \oplus k_i$ pour un certain $j \in [1; \ell]$. Remarquons que c'est équivalent à

$$x_{i-2}^{\ell+1} \oplus F_{i-1}(x_{i-1}^{\ell+1} \oplus k_{i-1}) = x_{i-2}^j \oplus F_{i-1}(x_{i-1}^j \oplus k_{i-1})\,.$$

Si $x_{i-1}^{\ell+1} \neq x_{i-1}^j$, alors cela se produit avec probabilité au plus 2^{-n} puisque F_{i-1} est uniformément aléatoire et indépendante de $\cap_{s\in S} A_s$. Si $x_{i-1}^{\ell+1} = x_{i-1}^j$, alors nécessairement $x_i^{\ell+1} \neq x_i^j$ puisque $x^{\ell+1}$ et x^j sont deux requêtes distinctes. [1] En sommant sur les $j \in [1; \ell]$, la probabilité de $\texttt{XColl}_i$ est au plus $\ell/2^n$. Le raisonnement est similaire pour la probabilité de $\texttt{XColl}'_i$, ce qui prouve le lemme. ■

Cela nous permet d'utiliser le lemme 5.6 pour majorer la probabilité que le coupling échoue.

Lemme 5.15. *Soit q_e un entier positif. Alors, pour tout uplet $x \in (\mathcal{I}_{2n})^{*q_e}$, on a :*

$$\|\mu_x - \mu^*\| \leq \sum_{t=\lfloor \frac{r-1}{2} \rfloor}^{\lfloor \frac{2r-2}{3} \rfloor} \frac{2^t}{t+1} \binom{r-t}{2r-2-3t} \frac{q_e^{t+1}}{2^{tn}}\,.$$

▽

Démonstration. En utilisant successivement le lemme du coupling (lemme 2.1), le lemme 5.10, et le lemme 5.6 combiné au lemme 5.14, on a (en appliquant le lemme 5.6 avec $r-1$ plutôt que r) :

$$\|\nu_\ell - \nu_\ell^*\| \leq \Pr[\texttt{Fail}] \leq \Pr\left[\bigcap_{i=1}^{r-2} (A_i \cup A_{i+1})\right] \leq \sum_{t=\lfloor \frac{r-1}{2} \rfloor}^{\lfloor \frac{2r-2}{3} \rfloor} \binom{r-t}{2r-2-3t} \left(\frac{2\ell}{2^n}\right)^t\,.$$

1. Remarquons que l'événement « $x_{i-1}^{\ell+1}$ et x_{i-1}^j sont distincts » dépend de $\cap_{s\in S} A_s$, de telle façon que l'événement « $x_i^{\ell+1} = x_i^j$ » n'est pas indépendant de $\cap_{s\in S} A_s$.

Ainsi, par le lemme 5.8, on voit que, pour tout uplet $x \in (\mathcal{I}_{2n})^{*q_e}$:

$$\begin{aligned}\|\mu_x - \mu^*\| \leq \sum_{\ell=0}^{q_e-1} \|\nu_\ell - \nu_\ell^*\| &\leq \sum_{t=\lfloor\frac{r-1}{2}\rfloor}^{\lfloor\frac{2r-2}{3}\rfloor} \binom{r-t}{2r-2-3t} \sum_{\ell=0}^{q_e-1} \left(\frac{2\ell}{2^n}\right)^t \\ &\leq \sum_{t=\lfloor\frac{r-1}{2}\rfloor}^{\lfloor\frac{2r-2}{3}\rfloor} \binom{r-t}{2r-2-3t} \left(\frac{2}{2^n}\right)^t \int_{\ell=0}^{q_e} \ell^t d\ell \\ &\leq \sum_{t=\lfloor\frac{r-1}{2}\rfloor}^{\lfloor\frac{2r-2}{3}\rfloor} \frac{2^t}{t+1} \binom{r-t}{2r-2-3t} \frac{q_e^{t+1}}{2^{tn}},\end{aligned}$$

ce qui prouve le lemme. ∎

Finalement, en combinant les lemmes 5.7 et 5.15, on obtient la majoration suivante pour la borne de sécurité NCPA d'un schéma de Luby-Rackoff :

Théorème 5.16. *Soit q_e un entier positif. Alors :*

$$\mathbf{Adv}^{\mathrm{ncpa}}_{\mathtt{LR}[n,r]}(q_e) \leq \sum_{t=\lfloor\frac{r-1}{2}\rfloor}^{\lfloor\frac{2r-2}{3}\rfloor} \frac{2^t}{t+1} \binom{r-t}{2r-2-3t} \frac{q_e^{t+1}}{2^{tn}}.$$ ♢

La borne est dominée par le terme correspondant à $t = \lfloor (r-1)/2 \rfloor$. En particulier, quand $r = 2r' + 1$, le coefficient de ce terme dominant est simplement $2^{r'}$ et le terme dominant est donc simplement $2^{r'} q_e^{r'+1}/2^{r'n}$. (Curieusement, c'est exactement la borne que nous obtenons pour un schéma d'Even-Mansour à r' tours.) Ainsi, face à un attaquant NCPA, le schéma de Luby-Rackoff est sûr jusqu'à $\mathcal{O}(2^{\frac{tn}{t+1}})$ requêtes avec $t = \lfloor (r-1)/2 \rfloor$.

Comparaison avec la borne de Hoang-Rogaway (HR). Dans [HR10], Hoang et Rogaway prouvent la majoration suivante pour la sécurité NCPA d'un schéma de Luby-Rackoff $\mathtt{LR}[n,r]$:

$$\mathbf{Adv}^{\mathrm{ncpa}}_{\mathtt{LR}[n,r]}(q_e) \leq \frac{4^t}{t+1} \frac{q_e^{t+1}}{2^{tn}} \quad \text{with} \quad t = \left\lfloor \frac{r}{3} \right\rfloor.$$

Brièvement, leur analyse de la probabilité de coupler est la suivante : ils montrent que la probabilité de ne pas coupler sur les trois premiers tours est au plus $4\ell/2^n$, et ils itèrent ce raisonement sur les trois tours suivants, etc. En fait, ils améliorent la borne de sécurité tous les trois tours. Notre analyse est plus fine : on obtient, à peu près, le même avantage tous les deux tours, améliorant ainsi significativement la borne de sécurité. Par exemple, pour trois tours, la borne de HR et notre borne montrent que l'avantage est majoré par $2q_e^2/2^n$ (ce qui est exactement la borne originale de Luby-Rackoff). Tandis que la borne de HR ne s'améliore pas pour cinq tours, la nôtre montre déjà que l'avantage est majoré par $4q_e^3/2^{2n}$. La borne de HR donne une sécurité en $\mathcal{O}(q_e^3/2^{2n})$ uniquement à partir du 6ème tour. Nous présentons une comparaison concrète des deux bornes (dans le cadre CCA, c'est-à-dire en ayant doublé les tours) en figure 5.4.

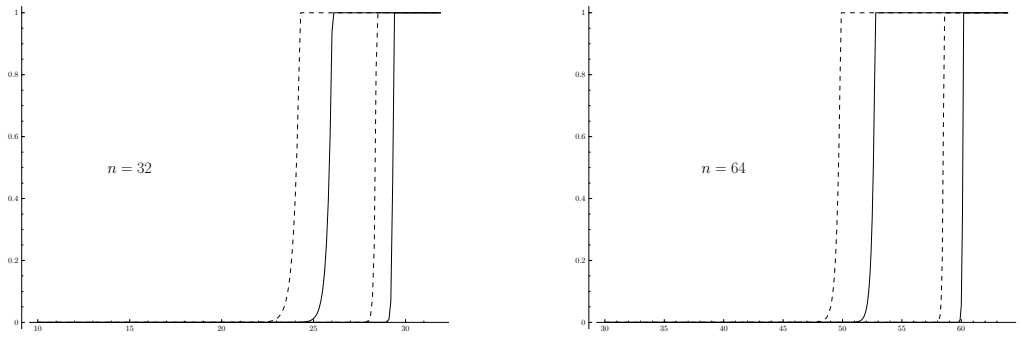

FIGURE 5.4 – Sécurité CCA pour le schéma de Luby-Rackoff $\texttt{LR}[n, r]$ en fonction de $\log_2(q_e)$, le log du nombre de requêtes de l'adversaire (à gauche : $n = 32$, à droite : $n = 64$). Les courbes en pointillés représentent la borne de Hoang-Rogaway [HR10], tandis que les courbes pleines représentent notre borne. Sur chaque graphe, les deux courbes les plus à gauche sont pour $r = 24$ et les deux plus à droite sont pour $r = 96$.

5.4 Indistinguabilité des schémas de Feistel à clés alternées face à une attaque CCA (étape 6)

5.4.1 Cas particulier du schéma de Luby-Rackoff

Afin de prouver la sécurité CCA, on utilise la stratégie classique de composer deux schémas NCPA-sûrs. On va utiliser le lemme suivant prouvé par Maurer, Renner et Pietrzak [MPR07] et Cogliati, Patarin et Seurin [CPS14].

Lemme 5.17 ([MPR07]). *Si G et H sont deux schémas de chiffrement par blocs avec le même domaine, alors, pour tout entier positif q, on a :*

$$\mathbf{Adv}^{\mathrm{cca}}_{H^{-1}\circ G}(q) \leq \mathbf{Adv}^{\mathrm{ncpa}}_{G}(q) + \mathbf{Adv}^{\mathrm{ncpa}}_{H}(q)\,,$$

où les clés de $H^{-1} \circ G$ sont choisies indépendantes entre les deux schémas H et G. ▽

Ce résultat n'est prouvé que dans le modèle standard où les schémas ne dépendent pas d'oracles additionnels, ce qui nous permet de n'utiliser ce lemme que pour le schéma de Luby-Rackoff.

Théorème 5.18. *Soit q_e un entier positif. Alors :*

$$\mathbf{Adv}^{\mathrm{cca}}_{\texttt{LR}[n,2r'-1]}(q_e) \leq \sum_{t=\lfloor \frac{r'-1}{2} \rfloor}^{\lfloor \frac{2r'-2}{3} \rfloor} \frac{2^{t+1}}{t+1} \binom{r'-t}{2r'-2-3t} \frac{q_e^{t+1}}{2^{tn}}\,.$$

♢

DÉMONSTRATION. Soit $\texttt{Rev}$ l'application « Reverse » définie par $\texttt{Rev}(x_L, x_R) = (x_R, x_L)$. Alors, comme déjà remarqué dans [MP03], un schéma de Feistel à $(2r' - 1)$ tours avec fonctions de tours $F_0, \ldots, F_{2r'-2}$ peut être écrit comme $\texttt{Rev} \circ H^{-1} \circ G$, où G et H sont des schémas de Feistel à r' tours. Cela peut être vu en écrivant la fonction de tour $F_{r'-1}$ comme le xor de deux fonctions de tours indépendantes $F'_{r'-1} \oplus F''_{r'-1}$ (clairement, cela ne change pas la distribution des sorties du système) : alors G est le schéma de Feistel avec

les fonctions de tours $F_0, \ldots, F_{r'-2}, F'_{r'-1}$ et H est le schéma de Feistel avec les fonctions de tours $F_{2r'-2}, \ldots, F_{r'}, F''_{r'-1}$. Le résultat se déduit en appliquant le lemme 5.17 et le théorème 5.16 (composer avec `Rev` ne modifie pas l'avantage). ∎

Pour un schéma de Luby-Rackoff à $2r'$ tours, on obtient la même borne que pour $2r'-1$ tours. A nouveau, la borne dans ce théorème est dominée par le terme correspondant à $t = \lfloor (r'-1)/2 \rfloor$. Ainsi, cela montre qu'un schéma de Luby-Rackoff à r tours assure une sécurité CCA jusqu'à $\mathcal{O}(2^{\frac{tn}{t+1}})$ requêtes, où $t = \left\lfloor \frac{\lfloor (r+1)/2 \rfloor - 1}{2} \right\rfloor = \lfloor \frac{r-1}{4} \rfloor$.

5.4.2 Cas général des KAF

Pour les KAF, puisqu'on ne peut pas appliquer le lemme 5.17 directement car le schéma fait appel à des oracles additionels, nous allons appliquer la même stratégie que pour le schéma d'Even-Mansour itéré qui repose sur le lemme suivant :

Lemme 5.19. *Soient $G^{\boldsymbol{F}}$ et $H^{\boldsymbol{F}'}$ deux schémas de chiffrement par blocs avec le même domaine, où $G^{\boldsymbol{F}}$ et $H^{\boldsymbol{F}'}$ dépendent respectivement des oracles $\boldsymbol{F} = (F_0, \ldots, F_{r-1})$ et $\boldsymbol{F}' = (F'_0, \ldots, F'_{r'-1})$ (cela peut être des oracles arbitraires, pas nécessairement des fonctions aléatoires). Supposons qu'il existe α_G tel que, pour tout uplet $x \in (\mathtt{MsgSp}(G))^{*q_e}$ et tout uplet $u = (u_0, \ldots, u_{r-1})$ et $v = (v_0, \ldots, v_{r-1})$ où $u_i \in (\mathcal{D}(F_i))^{q_f}$ et $v_i \in (\mathtt{Rng}(F_i))^{q_f}$, on a $\|\mu^G_{x,u,v} - \mu^*\| \leq \alpha_G$, et qu'il existe α_H tel que, pour tout uplet $x' \in (\mathtt{MsgSp}(H))^{*q_e}$ et tout uplet $u' = (u'_0, \ldots, u'_{r-1})$ et $v' = (v'_0, \ldots, v'_{r-1})$ où $u'_i \in (\mathcal{D}(F'_i))^{q_f}$ et $v'_i \in (\mathtt{Rng}(F'_i))^{q_f}$, on a $\|\mu^H_{x',u',v'} - \mu^*\| \leq \alpha_H$.*

(Ici, $\mathtt{MsgSp}(E)$ est le domaine de E, $\mathcal{D}(F)$ et $\mathtt{Rng}(F)$ sont respectivement le domaine et l'espace d'arrivée de l'oracle F, et les distributions sont définies comme en section 5.3.3, c'est-à-dire $\mu^G_{x,u,v}$ est la distribution des sorties de $G^{\boldsymbol{F}}$ après avoir reçu les entrées x, conditionné par $\boldsymbol{F}(u) = v$, et $\mu^H_{x',u',v'}$ est la distribution des sorties de $H^{\boldsymbol{F}'}$ après avoir reçu les entrées x', conditionné par $\boldsymbol{F}'(u') = v'$.)

Alors :

$$\mathbf{Adv}^{\mathrm{cca}}_{(H^{\boldsymbol{F}'})^{-1} \circ G^{\boldsymbol{F}}}(q_e, q_f) \leq 2(\sqrt{\alpha_G} + \sqrt{\alpha_H})\,. \qquad \triangledown$$

Démonstration. Notons $M = |\mathtt{MsgSp}(G)| = |\mathtt{MsgSp}(H)|$. Rappelons le résultat du lemme 3.8 :

Soit Ω un ensemble fini et ν la distribution uniforme sur Ω. Soit μ la distribution de probabilité sur Ω telle que $\|\mu - \nu\| \leq \varepsilon$. Alors, il existe un ensemble $S \subset \Omega$ tel que :

- $|S| \geq (1 - \sqrt{\varepsilon})|\Omega|$
- $\forall x \in S$, $\mu(x) \geq (1 - \sqrt{\varepsilon})\nu(x)$

En appliquant ce lemme à G et H, on déduit qu'il existe un sous-ensemble $S_x \subseteq (\mathtt{MsgSp}(G))^{*q_e}$ de taille supérieure ou égale à

$$(1 - \sqrt{\alpha_G})M(M-1)\cdots(M-q_e+1)$$

tel que, pour tout $z \in S_x$, on a :

$$\mu^G_{x,u,v}(z) \geq (1 - \sqrt{\alpha_G})\frac{1}{M(M-1)\cdots(M-q_e+1)}\,.$$

De manière similaire, il existe un sous-ensemble $S_y \subseteq (\mathtt{MsgSp}(H))^{*q_e}$ de taille supérieure ou égale à

$$(1 - \sqrt{\alpha_H})M(M-1)\cdots(M-q_e+1)$$

tel que, pour tout $z \in S_y$, on a :

$$\mu^H_{y,u',v'}(z) \geq (1-\sqrt{\alpha_H})\frac{1}{M(M-1)\cdots(M-q_e+1)}\,.$$

On peut maintenant minorer la probabilité que $(H^{\boldsymbol{F}'})^{-1} \circ G^{\boldsymbol{F}}(x) = y$ en sommant, sur toutes les valeurs intermédiaires $z \in S_x \cap S_y$, les probabilités que $G^{\boldsymbol{F}}(x) = z$ et $H^{\boldsymbol{F}'}(y) = z$. Plus précisément :

$$\begin{aligned}
&\Pr[\boldsymbol{F}(u) = v \wedge \boldsymbol{F}'(u') = v' \wedge (H^{\boldsymbol{F}'})^{-1} \circ G^{\boldsymbol{F}}(x) = y] \\
&\quad \geq \Pr[\boldsymbol{F}(u) = v \wedge \boldsymbol{F}'(u') = v'] \sum_{z \in S_x \cap S_y} \mu^G_{x,u,v}(z)\mu^H_{y,u',v'}(z) \\
&\quad \geq \Pr[\boldsymbol{F}(u) = v \wedge \boldsymbol{F}'(u') = v']\frac{|S_x \cap S_y|(1-\sqrt{\alpha_G})(1-\sqrt{\alpha_H})}{(M(M-1)\cdots(M-q_e+1))^2}\,.
\end{aligned}$$

Finalement, en remarquant que $|S_x \cap S_y| \geq (1-\sqrt{\alpha_G}-\sqrt{\alpha_H})M(M-1)\cdots(M-q_e+1)$, et en utilisant que

$$(1-\sqrt{\alpha_G}-\sqrt{\alpha_H})(1-\sqrt{\alpha_G})(1-\sqrt{\alpha_H}) \geq 1-2(\sqrt{\alpha_G}+\sqrt{\alpha_H})\,,$$

on vérifie que :

$$\begin{aligned}
\Pr[\boldsymbol{F}(u) = v \wedge \boldsymbol{F}'(u') = v' \wedge (H^{\boldsymbol{F}'})^{-1} \circ G^{\boldsymbol{F}}(x) = y] \geq \\
(1-\beta)\frac{Pr[\boldsymbol{F}(u) = v \wedge \boldsymbol{F}'(u') = v']}{M(M-1)\cdots(M-q_e+1)}
\end{aligned}$$

où $\beta = 2(\sqrt{\alpha_G}+\sqrt{\alpha_H})$. Pour finir, en adaptant le lemme 3.5 au cas des KAF et en remarquant que

$$\frac{Pr[\boldsymbol{F}(u) = v \wedge \boldsymbol{F}'(u') = v']}{M(M-1)\cdots(M-q_e+1)} = \Pr^*\left[\boldsymbol{F}(u) = v \wedge \boldsymbol{F}'(u') = v' \wedge P(x) = y\right]\,,$$

où P est une permutation uniformément aléatoire et indépendante de $\boldsymbol{F}$ et $\boldsymbol{F}'$, on déduit que :

$$\mathbf{Adv}^{\mathrm{cca}}_{(H^{\boldsymbol{F}'})^{-1}\circ G^{\boldsymbol{F}}}(q_e, q_f) \leq 2(\sqrt{\alpha_G}+\sqrt{\alpha_H})\,. \qquad \blacksquare$$

Ainsi, nous obtenons la majoration suivante pour la sécurité CCA d'un KAF à $2r'$ tours :

Théorème 5.20. *Soient q_e, q_f des entiers positifs. Alors :*

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathtt{KAF}[n,2r']}(q_e, q_f) \leq 4\left(\frac{4^t}{t+1}\frac{(q_e+2q_f)^{t+1}}{2^{tn}}\right)^{1/2} \quad \text{avec} \quad t = \left\lfloor \frac{r'}{3} \right\rfloor\,. \qquad \diamondsuit$$

Démonstration. Puisque dans ce contexte, le distingueur a accès aux fonctions de tours internes, on ne peut pas utiliser l'astuce d'écrire la fonction de tour du milieu d'un schéma à $2r'-1$ tours comme le xor de deux fonctions indépendantes. Considérons donc un KAF à $2r'$ tours. Tout d'abord, on remarque que tous les résultats de la section 5.3.5 s'appliquent, de la même manière, à l'inverse d'un KAF. Ainsi, on peut voir un KAF à $2r'$ tours comme la composition d'un KAF à r' tours et l'inverse de l'inverse d'un KAF à r' tours indépendant du premier. Le résultat se déduit en combinant les lemmes 5.19 et 5.12. $\blacksquare$

Pour un KAF à $(2r'+1)$ tours, on obtient la même borne qu'un KAF à $2r'$ tours. Ainsi, un KAF à r tours est CCA sûr jusqu'à $\mathcal{O}(2^{\frac{tn}{t+1}})$ requêtes au total, où $t = \left\lfloor \frac{\lfloor r/2 \rfloor}{3} \right\rfloor = \lfloor \frac{r}{6} \rfloor$.

Chapitre 6

Réductions du schéma d'Even-Mansour itéré à 2 tours

Dans ce chapitre, nous étudions les réductions possibles du schéma d'Even-Mansour itéré à 2 tours. Contrairement aux autres chapitres, ici, nous n'utiliserons pas la technique du coupling mais d'autres techniques comme les coefficients H, les sommes de Gauss et l'analyse de Fourier. Le coupling permet habituellement de prouver des bornes de sécurité pour un nombre arbitraire de tours mais il ne peut être utilisé quand l'aléa n'est pas renouvelé d'un tour à l'autre (ce qui est le cas si l'on prend des clés identiques). Dans ce cas là, au lieu d'étudier séparément des problèmes combinatoires simples pour ensuite les combiner, il s'agit d'étudier un problème combinatoire « indivisible » à l'aide de techniques plus puissantes comme l'analyse de Fourier. Les résultats présentés dans ce chapitre ont fait l'objet d'un article (Shan Chen, Rodolphe Lampe, Jooyoung Lee, Yannick Seurin et John P. Steinberger [CLL+14]) présenté à CRYPTO 2014.

6.1 Introduction

Dans tout ce chapitre, nous ne considérerons que des attaques CCA car nos preuves n'ont pas besoin, contrairement aux preuves par coupling, de considérer une étape où l'on analyse la sécurité face à une attaque NCPA.

6.1.1 Objectif

Rappelons les résultats sur les preuves de sécurité du schéma d'Even-Mansour itéré pour les premiers tours. Pour $r = 1$, on sait que le schéma d'Even-Mansour à une clé $x \mapsto k \oplus P(k \oplus x)$ assure une sécurité jusqu'à $\mathcal{O}(2^{n/2})$ requêtes, où n est le nombre de bits de la clé et des blocs. Comme l'ont remarqué Dunkelman *et al.* [DKS12], cette construction est « minimale » au sens où, si l'on enlève une addition ou la permutation, la construction devient trivialement distinguable d'une permutation aléatoire. Pour deux tours, la meilleure preuve de sécurité de [CS14] nécessite deux permutations indépendantes P_1 et P_2, et deux clés indépendantes (k, k') pour construire trois clés indépendantes deux à deux, par exemple $(k, k' \oplus k, k')$. Elle permet de construire le schéma de chiffrement par blocs $x \mapsto k' \oplus P_2((k' \oplus k) \oplus P_1(k \oplus x))$ qui est sûr jusqu'à $\mathcal{O}(2^{2n/3})$ requêtes.

Dans ce chapitre, nous souhaitons répondre au problème suivant :

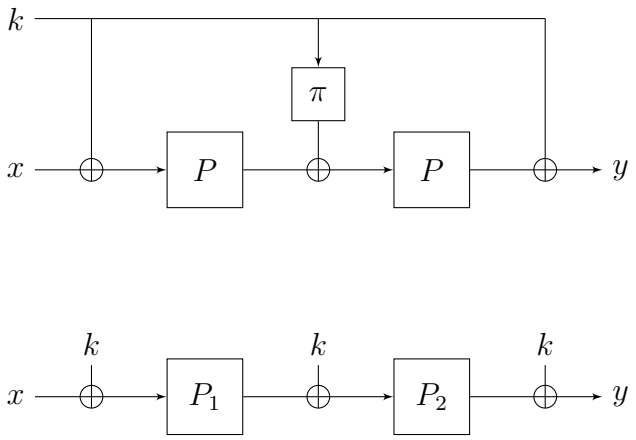

FIGURE 6.1 – Deux constructions d'un schéma d'Even-Mansour itéré à deux tours « minimaux » et sûr jusqu'à $\widetilde{\mathcal{O}}(2^{\frac{2n}{3}})$ requêtes de n'importe quel attaquant CCA. En haut : π est un orthomorphisme linéaire fixé de $\mathbb{F}_2^n$, et P est une permutation aléatoire publique. En bas : P_1 et P_2 sont deux permutations aléatoires publiques indépendantes.

> *Peut-on obtenir une sécurité jusqu'à $\mathcal{O}(2^{2n/3})$ requêtes, similaire à celle obtenue avec le schéma d'Even-Mansour itéré à deux tours (avec deux clés indépendantes et deux permutations indépendantes), avec juste une clé k et/ou une permutation P ?*

Cette question est naturelle car la plupart des schémas de chiffrement basés sur la structure SPN ont des clés de tours qui dérivent d'une clé principale de n bits (ou, plus généralement, une clé de ℓ bits où $\ell \in [n, 2n]$ est petit par rapport à la taille totale des clés de tours), et utilisent la même permutation, ou des permutations très proches, à chaque tour. Il est donc fondamental de déterminer si la sécurité s'améliore avec le nombre de tours même si l'on utilise la même clé et/ou la même permutation.

6.1.2 Résultat

Nous répondons positivement à la question précédente. Notre théorème principal établit les conditions suffisantes pour obtenir trois clés (k_0, k_1, k_2) de n bits dérivant d'une clé principale k de n bits de telle façon que le schéma d'Even-Mansour itéré à deux tours avec une seule permutation

$$x \mapsto k_2 \oplus P(k_1 \oplus P(k_0 \oplus x))$$

soit sûr jusqu'à $\widetilde{\mathcal{O}}(2^{2n/3})$ requêtes, où la notation $\widetilde{\mathcal{O}}(\cdot)$ ne tient pas compte des facteurs logarithmiques (en $N = 2^n$). En particulier, une telle dérivation de clé $k \mapsto (k_0, k_1, k_2)$ peut être construite à l'aide de n'importe quel orthomorphisme de $\mathbb{F}_2^n$. Une permutation π de $\{0,1\}^n$ est appelée orthomorphisme si $x \mapsto x \oplus \pi(x)$ est aussi une permutation. Les bonnes propriétés cryptographiques des orthomorphismes ont déjà été remarquées (par exemple [Mit95, GGM99]), et en particulier utilisées pour les constructions de Lai-Massey [LM90, Vau99] telles que les schémas de chiffrement par blocs IDEA [LM90] et FOX [JV04]. Notre théorème principal est le suivant :

Théorème (informel). *Soit π un orthomorphisme linéaire fixé de $\mathbb{F}_2^n$, et P une permutation aléatoire publique. Alors, le schéma de chiffrement par blocs* EMSP *ayant pour domaine et pour espace des clés $\{0,1\}^n$ et défini par (voir figure 6.1)*

$$\mathsf{EMSP}_k^P(x) = k \oplus P(\pi(k) \oplus P(k \oplus x)) \qquad (\star)$$

est sûr jusqu'à $\widetilde{\mathcal{O}}(2^{\frac{2n}{3}})$ requêtes à EMSP_k^P et P. (Les requêtes peuvent être adaptatives et dans les deux directions pour E_k^P et P).

Nous remarquons qu'en supprimant π de la construction ($\star$), c'est-à-dire si on ajoute la même clé k chaque fois, la sécurité est dégradée à $\mathcal{O}(2^{n/2})$ requêtes. Plus généralement, si les clés de tours sont égales et la même permutation P est utilisée à chaque tour, la sécurité est dégradée à $\mathcal{O}(2^{n/2})$ requêtes, indépendamment du nombre de tours r. Cela semble être un résultat standard des « slide attacks » [BW99, BW00], mais nous n'avons pas trouvé de preuves détaillées dans la littérature et nous présenterons et analyserons donc ce résultat dans ce chapitre. Nous présenterons également une variante dans le cas d'une clé, qui consiste à xorer des constantes aux clés de tours. Ainsi, la construction ($\star$) peut être vue comme un schéma d'Even-Mansour itéré à deux tours « minimal » assurant une sécurité au delà de la borne des anniversaires puisqu'en supprimant n'importe quelle opération, la sécurité est dégradée à $\mathcal{O}(2^{n/2})$ requêtes au mieux (pour π, cela vient de l'attaque que nous venons de mentionner, et pour n'importe quelle instance de P, cela revient à analyser la sécurité d'un schéma d'Even-Mansour à un tour). De plus, nous montrerons qu'en utilisant deux permutations aléatoires publiques indépendantes P_1 et P_2, la dérivation de clé triviale est suffisante (c'est-à-dire ajouter la même clé k à chaque tour, voir figure 6.1) : le schéma ainsi défini est sûr jusqu'à $\widetilde{\mathcal{O}}(2^{2n/3})$ requêtes.

A notre connaissance, ce sont les premiers résultats prouvant une sécurité au delà de la borne des anniversaires pour le schéma d'Even-Mansour itéré et qui ne reposent pas sur la condition d'indépendance des clés de tours. Cela permet de mieux cerner les propriétés nécessaires pour construire les clés de tours. En particulier, il semble qu'une dérivation de clé pseudo-aléatoire ne soit pas nécessaire. Néanmoins, nous rappelons que notre résultat se place dans le modèle idéalisé de la permutation aléatoire et n'assure donc pas la sécurité du schéma une fois que les permutations internes sont instanciées. On sait en revanche que toute attaque nécessitant moins de requêtes que celles que nous obtenons, dans le modèle de la permutation aléatoire, doit exploiter les faiblesses de la permutation instanciée.

6.1.3 Techniques employées

Afin de prouver notre résultat principal, nous nous plaçons, exactement comme nous l'avons fait dans les chapitres précédents, dans le cadre d'un distingueur qui cherche à distinguer deux mondes : le monde « réel » (EMSP_k^P, P), où EMSP_k^P est le schéma d'Even-Mansour itéré à deux tours, une permutation P et une clé k, et le monde « idéal » (E, P) où E est une permutation uniformément aléatoire et indépendante de P. Le distingueur peut faire au plus q_e requêtes à EMSP_k^P/E et au plus q_p requêtes à P (toutes les requêtes peuvent être adaptatives et directes ou inverses, et l'attaquant a, comme d'habitude, une capacité de calcul non bornée). Contrairement à ce que nous avons fait dans les chapitres précédents, nous n'allons pas utiliser ici le coupling pour majorer l'avantage du distingueur. Nous utiliserons ici la technique des coefficients H de Jacques Patarin [Pat91, Pat08]. Cette technique consiste, entre autre, à partitionner l'ensemble des transcriptions possibles de l'interaction entre le distingueur et les oracles de permutations : un ensemble $\mathcal{T}_1$ de

« bonnes » transcriptions et un ensemble $\mathcal{T}_2$ de « mauvaises » transcriptions. Les bonnes transcriptions $\tau \in \mathcal{T}_1$ vérifient la propriété que le rapport entre les probabilités d'obtenir τ dans le monde réel et d'obtenir τ dans le monde idéal est supérieur à $1 - \varepsilon_1$ pour une certaine valeur $\varepsilon_1 > 0$, tandis que la probabilité d'obtenir de mauvaises transcriptions $\tau \in \mathcal{T}_2$ (dans le monde idéal) est inférieure à une certaine valeur $\varepsilon_2 > 0$. Alors l'avantage du distingueur peut être majoré par $\varepsilon_1 + \varepsilon_2$.

Afin de développer une intuition à propos des bonnes et mauvaises transcriptions, regardons comment un attaquant peut être « chanceux » lors d'une attaque. Plus précisément, considérons l'attaque suivante (pour simplifier, on suppose $q_e = q$ et $q_p = 2q$) : le distingueur $\mathcal{D}$ commence par faire q requêtes arbitraires à la permutation externe EMSP_k^P/E et en déduit un ensemble de q paires $\mathcal{Q}_E = \{(x_1, y_1), \ldots, (x_q, y_q)\}$; puis, $\mathcal{D}$ détermine la paire d'ensembles (U, V) avec $|U| = |V| = q$ et $U, V \subseteq \{0,1\}^n$, qui maximisent la taille de l'ensemble

$$\mathcal{K}(\mathcal{Q}_E, U, V) \stackrel{\text{def}}{=} \{k' \in \{0,1\}^n : \exists (x_i, y_i) \in \mathcal{Q}_E \text{ tels que } x_i \oplus k' \in U, y_i \oplus k' \in V\} \subseteq \{0,1\}^n, \tag{6.1}$$

et $\mathcal{D}$ fait les requêtes $P(u)$, $P^{-1}(v)$ pour tout $u \in U$, $v \in V$. Remarquons que, si $\mathcal{D}$ est dans le monde réel et si la clé k appartient à l'ensemble $\mathcal{K}(\mathcal{Q}_E, U, V)$, alors $\mathcal{D}$ peut vérifier qu'une de ses requêtes à EMSP_k^P/E est compatible avec deux de ses requêtes à P en accord avec k. En effet, il existe i et les requêtes (u, v), (u', v') à P telles que $x_i \oplus k = u$, $v \oplus \pi(k) = u'$, et $v' \oplus k = y_i$. Un tel cycle ne peut se produire que pour un faible nombre de clés de $\mathcal{K}(\mathcal{Q}_E, U, V)$, de telle façon que de « fausses alertes » (des clés qui vérifient un tel cycle sans être la clé k utilisée par le schéma) peuvent facilement être écartées en testant d'autres requêtes. La clé k, à condition d'appartenir à $\mathcal{K}(\mathcal{Q}_E, U, V)$, peut donc être rapidement trouvée. De plus, des considérations heuristiques laissent supposer que k appartient à $\mathcal{K}(\mathcal{Q}_E, U, V)$ avec probabilité $|\mathcal{K}(\mathcal{Q}_E, U, V)|/2^n$. Il devient donc nécessaire de prouver que $|\mathcal{K}(\mathcal{Q}_E, U, V)|$ est significativement plus petit que 2^n avec une probabilité forte sur $\mathcal{Q}_E$. Il s'agit donc de montrer que

$$\max_{\substack{U,V \subseteq \{0,1\}^n \\ |U|=|V|=q}} |\{k' \in \{0,1\}^n : \exists (x_i, y_i) \in \mathcal{Q}_E \text{ s.t. } x_i \oplus k' \in U, y_i \oplus k' \in V\}| \tag{6.2}$$

est significativement plus petit que 2^n avec une probabilité forte sur $\mathcal{Q}_E$ pour prouver que $\mathcal{D}$ a un avantage faible. L'un des critères qui rend une transcription « mauvaise » dans notre preuve est le fait que l'ensemble de requêtes $\mathcal{Q}_E$ à EMSP_k^P/E est tel que (6.2) est plus grand que désiré. (Par la suite, $\mathcal{K}(\mathcal{Q}_E, U, V)$ sera noté BadK_1 dans les définitions 6.1 et 6.2 d'une mauvaise transcription.)

Remarquons que

$$\begin{aligned} |\mathcal{K}(\mathcal{Q}_E, U, V)| &\leq |\{(k', u, v) \in \{0,1\}^n \times U \times V : k' \oplus u = x_i, k' \oplus v = y_i \text{ pour } 1 \leq i \leq q\}| \\ &= |\{(i, u, v) \in \{1, \ldots, q\} \times U \times V : x_i \oplus y_i = u \oplus v\}|. \end{aligned}$$

Remarquons également que l'ensemble de valeurs $\{x_i \oplus y_i : (x_i, y_i) \in \mathcal{Q}_E\}$ est essentiellement aléatoire puisque, si la i-ème requête à EMSP_k^P/E est directe, alors y_i est aléatoire dans un grand ensemble, tandis que x_i est aléatoire dans un grand ensemble si la requête est inverse. De plus, le problème de majorer

$$\mu(A) \stackrel{\text{def}}{=} \max_{\substack{U,V \subseteq \{0,1\}^n \\ |U|=|V|=q}} |\{(a, u, v) \in A \times U \times V : a = u \oplus v\}$$

pour un ensemble $A \subseteq \{0,1\}^n$ *purement aléatoire* de taille q a déjà été étudié avant [Bab89, Hay05, AKKR08, KPS13, Ste13], il est appelé *sum-capture problem* [Ste13]. L'un des résultats principaux [Bab89, Ste13] sur le sum-capture problem est que $\mu(A)$ est majoré par, approximativement, $q^{3/2}$ pour $q \leq 2^{2n/3}$. De manière surprenante, c'est exactement la borne suffisante pour prouver notre résultat puisque $q^{3/2} \ll 2^n$ pour $q \ll 2^{2n/3}$. (Ce qui implique alors que (6.2) est loin de 2^n si q reste inférieur à $2^{2n/3}$, comme voulu.) Nos hypothèses sont, en revanche, légèrement différentes car l'ensemble $\{x_i \oplus y_i : (x_i, y_i) \in \mathcal{Q}_E\}$ n'est pas, contrairement à A, un ensemble purement aléatoire. D'autres complications s'ajoutent : dans le cas général où les trois clés (k_0, k_1, k_2) dérivent d'une clé principale k de n bits en utilisant les fonctions (bijectives) de dérivation $\gamma_i : k \mapsto k_i$, $\mathcal{K}(\mathcal{Q}_E, U, V)$ s'écrit alors

$$\{k' \in \{0,1\}^n : \exists (x_i, y_i) \in \mathcal{Q}_E \text{ tel que } x_i \oplus \gamma_0(k') \in U, y_i \oplus \gamma_2(k') \in V\},$$

de telle façon que nous devons majorer par

$$\left|\{(i,u,v) \in \{1,\ldots,q\} \times U \times V : x_i \oplus u = \gamma_0 \circ \gamma_2^{-1}(y_i \oplus v)\}\right|.$$

Nous devons donc adapter (et parfois étendre) les techniques d'analyse de Fourier utilisées dans [Bab89, Ste13].

Une fois que la probabilité d'obtenir une mauvaise transcription est majorée, la seconde partie de la preuve consiste à montrer que le rapport entre les probabilités d'obtenir une bonne transcription dans le monde réel et dans le monde idéal est proche de 1. Cela consiste principalement en un argument combinatoire. Quand les permutations sont indépendantes (figure 6.1), l'argument n'est pas extrêmement compliqué et nous le présentons en section 6.5 (voir lemme 6.13), ce qui est un bon point de départ avant de s'attaquer à la preuve plus compliquée pour le cas d'une seule permutation pour chaque tour. Dans ce cas là, il s'agira d'élargir les conditions d'une mauvaise transcription et l'argument combinatoire sera plus complexe. Cette partie est reliée au problème de distinguer $P \circ P$ (où P est uniformément aléatoire) d'une permutation uniformément aléatoire E.

6.1.4 Organisation

Nous commençons en section 6.2 par introduire quelques notations, définir le schéma d'Even-Mansour généralisé, rappeler les définitions de sécurité dans le modèle de la permutation aléatoire, rappeler la technique des coefficients H et enfin prouver certains résultats combinatoires utiles pour nos preuves. Dans la section 6.3, qui peut être lue et comprise indépendamment des autres sections, nous prouvons un nouveau résultat sur le sum-capture problem. En section 6.4, nous détaillons les « slide attacks » contre le schéma d'Even-Mansour généralisé à une permutation et une clé. Les sections 6.5 et 6.6 présentent nos deux preuves de sécurité pour les deux variantes « minimales » du schéma d'Even-Mansour généralisé à 2 tours (voir figure 6.1).

6.2 Préliminaires

6.2.1 Notations

Permutations

Comme d'habitude, on fixe un entier $n \geq 1$, et $N = 2^n$. Etant donné $\mathcal{Q} = ((x_1, y_1), \ldots, (x_q, y_q))$, où les x_i sont des éléments de $\mathcal{I}_n$ deux à deux distincts, les y_i des éléments de $\mathcal{I}_n$ deux à

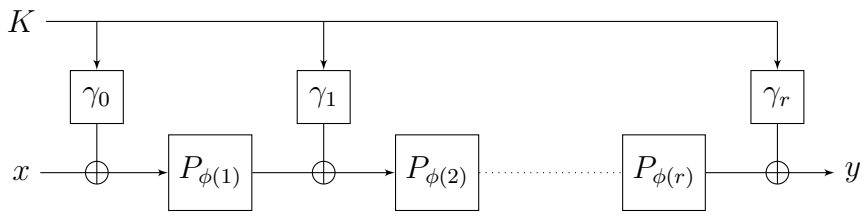

FIGURE 6.2 – Le schéma d'Even-Mansour généralisé à r tours.

deux distincts, et une permutation $P \in \mathcal{P}_n$, on dit que P prolonge $\mathcal{Q}$, qu'on note $P \vdash \mathcal{Q}$, si $P(x_i) = y_i$ pour $i = 1, \ldots, q$. Soit $X = \{x \in \{0,1\}^n : (x,y) \in \mathcal{Q}\}$ et $Y = \{y \in \{0,1\}^n : (x,y) \in \mathcal{Q}\}$. On appelle X et Y respectivement le domaine et l'espace d'arrivée de $\mathcal{Q}$. Par abus de notation, on notera parfois $\mathcal{Q}$ la bijection de X dans Y telle que $\mathcal{Q}(x_i) = y_i$ pour $i = 1, \ldots, q$. Ainsi, pour tout $X' \subseteq X$, on a $\mathcal{Q}(X') = \{y \in \{0,1\}^n : (x,y) \in \mathcal{Q} \wedge x \in X'\}$, et pour tout $Y' \subseteq Y$, on a $\mathcal{Q}^{-1}(Y') = \{x \in \{0,1\}^n : (x,y) \in \mathcal{Q} \wedge y \in Y'\}$. Nous utiliserons souvent le fait suivant : étant donné $\mathcal{Q}$ de taille q et $\mathcal{Q}'$ de taille q', de domaines respectifs X et X' et d'espaces d'arrivée respectifs Y et Y' vérifiant $X \cap X' = \emptyset$ et $Y \cap Y' = \emptyset$, on a :

$$\Pr\left[P \leftarrow_{\$} \mathcal{P}_n : P \vdash \mathcal{Q}' \,\middle|\, P \vdash \mathcal{Q}\right] = \frac{1}{(N-q)_{q'}}\,.$$

Quand deux ensembles A et B sont disjoints, on note $A \sqcup B$ leur union disjointe.

Espace vectoriel $\mathbb{F}_2^n$

On note $\mathbb{F}_2 \simeq \{0,1\}$ le corps à 2 éléments et $\mathbb{F}_2^n$ l'espace vectoriel de dimension n sur $\mathbb{F}_2$. Etant donné deux vecteurs $x = (x_1, \ldots, x_n)$ et $y = (y_1, \ldots, y_n)$ de $\mathbb{F}_2^n$, on note $x \cdot y = \sum_{i=1}^n x_i y_i \bmod 2$ le produit scalaire de x et y. Le groupe linéaire de degré n sur $\mathbb{F}_2$, c'est-à-dire l'ensemble de tous les automorphismes (les bijections linéaires) de $\mathbb{F}_2^n$, est noté $\mathsf{GL}(n)$. Etant donné $\Gamma \in \mathsf{GL}(n)$, on note Γ^* l'adjoint de Γ, c'est-à-dire l'unique automorphisme vérifiant $x \cdot \Gamma(y) = \Gamma^*(x) \cdot y$ pour tout $x, y \in \mathbb{F}_2^n$.

6.2.2 Le schéma d'Even-Mansour généralisé

Fixons des entiers $n, r, m, \ell \geq 1$. Soit $\phi : \{1, \ldots, r\} \to \{1, \ldots, m\}$ une fonction arbitraire et $\boldsymbol{\gamma} = (\gamma_0, \ldots, \gamma_r)$ un uplet de $r+1$ fonctions de $\{0,1\}^\ell$ dans $\{0,1\}^n$. A partir de n'importe quel uplet de m permutations $\boldsymbol{P} = (P_1, \ldots, P_m)$ de $\{0,1\}^n$, le schéma d'Even-Mansour généralisé à r tours $\mathsf{EMSP}[n, r, m, \ell, \phi, \boldsymbol{\gamma}]$ est définit comme le schéma de chiffrement par blocs ayant pour domaine $\{0,1\}^n$ et pour espace des clés $\{0,1\}^\ell$, noté $\mathsf{EMSP}^{\boldsymbol{P}}$ par la suite (les paramètres $[n, r, m, \ell, \phi, \boldsymbol{\gamma}]$ sont implicites et déduits du contexte), qui envoie un message $x \in \{0,1\}^n$ et une clé $K \in \{0,1\}^\ell$ sur le chiffré défini par (voir figure 6.2) :

$$\mathsf{EMSP}^{\boldsymbol{P}}(K,x) = \gamma_r(K) \oplus P_{\phi(r)}(\gamma_{r-1}(K) \oplus P_{\phi(r-1)}(\cdots P_{\phi(2)}(\gamma_1(K) \oplus P_{\phi(1)}(\gamma_0(K) \oplus x)) \cdots))\,.$$

On note $\mathsf{EMSP}^{\boldsymbol{P}}_K : x \mapsto \mathsf{EMSP}^{\boldsymbol{P}}(K,x)$ le schéma d'Even-Mansour généralisé instancié avec la clé K (ainsi, $\mathsf{EMSP}^{\boldsymbol{P}}_K$ est une permutation sur $\{0,1\}^n$).

Par exemple, l'AES-128 est un schéma d'Even-Mansour généralisé où $n = 128$, $r = 10$, $m = 2$, $\ell = 128$, la fonction ϕ est définie par $\phi(i) = 1$ pour $i = 1, \ldots, 9$ et $\phi(10) = 2$,

chaque fonction de dérivation de clé γ_i est une permutation (non linéaire pour $i \geq 1$) sur $\{0,1\}^{128}$, et les permutations P_1 et P_2 sont définies comme :

$$P_1 = \mathsf{MixColumns} \circ \mathsf{ShiftRows} \circ \mathsf{SubBytes}$$
$$P_2 = \mathsf{ShiftRows} \circ \mathsf{SubBytes}\,.$$

Nous allons nous intéresser aux deux cas particuliers suivants :

– le cas où les permutations sont indépendantes et la même clé k de n bits est utilisée à chaque tour, c'est-à-dire $m = r$, ϕ est l'identité, $\ell = n$, et tous les γ_i sont l'identité, auquel cas, on notera $\mathsf{EMIP}[n, r]$ le schéma résultant. Ainsi, pour un uplet de r permutations $\boldsymbol{P} = (P_1, \ldots, P_r)$, le schéma $\mathsf{EMIP}^{\boldsymbol{P}}$ envoie un message $x \in \{0,1\}^n$ et une clé $k \in \{0,1\}^n$ sur le chiffré défini par :

$$\mathsf{EMIP}^{\boldsymbol{P}}(k, x) = k \oplus P_r(k \oplus P_{r-1}(\cdots P_2(k \oplus P_1(k \oplus x)) \cdots))\,.$$

– le cas où une même permutation P est utilisée à chaque tour, c'est-à-dire $m = 1$ et $\phi(i) = 1$ pour $i = 1, \ldots, r$, auquel cas, on notera $\mathsf{EMSP}[n, r, \ell, \boldsymbol{\gamma}]$ le schéma résultant. Ainsi, pour une permutation P, le schéma EMSP^P envoie un message $x \in \{0,1\}^n$ et une clé $K \in \{0,1\}^\ell$ sur le chiffré défini par :

$$\mathsf{EMSP}^P(K, x) = \gamma_r(K) \oplus P(\gamma_{r-1}(K) \oplus P(\cdots P(\gamma_1(K) \oplus P(\gamma_0(K) \oplus x)) \cdots))\,.$$

Quand $\ell = n$ (c'est-à-dire quand la taille de la clé principale est égale à la taille des blocs), on notera $\mathsf{EMSP}[n, r, \boldsymbol{\gamma}]$ le schéma correspondant.

6.2.3 Indistinguabilité

On rappelle brièvement les définitions d'avantage et d'indistinguabilité. Ces définitions sont similaires aux définitions déjà présentées dans les chapitres précédents. On considère un distingueur $\mathcal{D}$ qui interagit avec un ensemble de $m+1$ oracles de permutation de $\mathcal{P}_n$ qu'on note $(P_0, P_1 \ldots, P_m) = (P_0, \boldsymbol{P})$. Le but de $\mathcal{D}$ est de distinguer si il interagit avec $(\mathsf{EMSP}_K^{\boldsymbol{P}}, \boldsymbol{P})$, où $\boldsymbol{P} = (P_1, \ldots, P_m)$ est un uplet de permutations uniformément aléatoires et indépendantes et K est uniformément aléatoire dans $\{0,1\}^\ell$ (le monde dit « réel »), ou avec $(E, \boldsymbol{P})$, où E est une permutation uniformément aléatoire et indépendante de $\boldsymbol{P}$ (le monde dit « idéal »). La première permutation E est dite externe tandis que les permutations $P_1, \ldots, P_m$ sont dites internes. Le distingueur est adaptatif et peut faire des requêtes directes et inverses, ce qui correspond à une attaque CCA. Comme d'habitude, on considère des distingueurs qui ont des capacités de calcul non bornées, déterministes et qui ne font pas de requêtes redondantes.

L'avantage de $\mathcal{D}$ est défini par :

$$\mathbf{Adv}(\mathcal{D}) = \left|\Pr\left[\mathcal{D}^{\mathsf{EMSP}_K^{\boldsymbol{P}}, \boldsymbol{P}} = 1\right] - \Pr\left[\mathcal{D}^{E, \boldsymbol{P}} = 1\right]\right|,$$

où la première probabilité est prise sur les choix aléatoires de K et $\boldsymbol{P}$, et la seconde probabilité sur les choix aléatoires de E et $\boldsymbol{P}$.

Pour q_e, q_p des entiers positifs, on définit l'avantage CCA pour distinguer le schéma d'Even-Mansour généralisé d'une permutation aléatoire par :

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{EMSP}[n,r,m,\ell,\phi,\boldsymbol{\gamma}]}(q_e, q_p) = \max_{\mathcal{D}} \mathbf{Adv}(\mathcal{D})\,,$$

où le maximum est pris sur tous les distingueurs $\mathcal{D}$ faisant exactement q_e requêtes à la permutation externe et q_p requêtes à chaque permutation interne.

6.2.4 La technique des coefficients H

On rappelle ici la technique des coefficients H et les notations que nous utiliserons pour manipuler les transcriptions de l'interaction entre le distingueur et les oracles.

Transcriptions

Toutes les informations récupérées par le distingueur durant l'interaction avec le système de $m+1$ permutations peuvent être résumées par la transcription de cette interaction, c'est-à-dire la liste ordonnée des requêtes et des réponses reçues. On note chaque requête et sa réponse par un uplet (i, b, z, z'), où $i \in \{0, \ldots, m\}$ correspond au numéro de la permutation qui fait l'objet de la requête, b est un bit indiquant le sens de la requête (0 pour une requête directe et 1 pour une requête inverse), $z \in \{0,1\}^n$ est la requête faite à P_i et z' la réponse. On dit qu'une transcription est *atteignable* (en fonction d'un distingueur fixé $\mathcal{D}$) si il existe un uplet de permutations $(P_0, \ldots, P_m) \in (\mathcal{P}_n)^{m+1}$ tel que l'interaction de $\mathcal{D}$ avec $(P_0, \ldots, P_m)$ produit la transcription (autrement dit, la probabilité d'obtenir la transcription dans le monde « idéal » est non-nulle). En fait, une transcription atteignable peut être représentée d'une façon plus pratique : à partir d'une transcription, on construit $m+1$ listes :

$$\begin{aligned}
\mathcal{Q}_E &= ((x_1, y_1), \ldots, (x_{q_e}, y_{q_e}))\,, \\
\mathcal{Q}_{P_1} &= ((u_{1,1}, v_{1,1}), \ldots, (u_{1,q_p}, v_{1,q_p}))\,, \\
&\vdots \\
\mathcal{Q}_{P_m} &= ((u_{m,1}, v_{m,1}), \ldots, (u_{m,q_p}, v_{m,q_p}))
\end{aligned}$$

de la manière suivante. Pour $j = 1, \ldots, q_e$, soit $(0, b, z, z')$ la j-ème requête à P_0 dans la transcription : si c'est une requête directe alors on fixe $x_j = z$ et $y_j = z'$, sinon on fixe $x_j = z'$ et $y_j = z$. De la même manière, pour chaque $i = 1, \ldots, m$, et $j = 1, \ldots, q_p$, soit (i, b, z, z') la j-ème requête à P_i dans la transcription : si c'est une requête directe alors on fixe $u_{i,j} = z$ et $v_{i,j} = z'$, sinon on fixe $u_{i,j} = z'$ et $v_{i,j} = z$. Il est assez clair que que, pour les transcriptions atteignables, il y a une bijection entre ces deux représentations. Essentiellement, cela vient du fait que le distingueur est déterministe. De plus, bien que nous ayons défini $\mathcal{Q}_E, \mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_m}$ comme des listes ordonnées, l'ordre n'a aucune importance (notre formalisation conserve l'ordre naturel induit par le distingueur).

Par commodité, en suivant [CS14], nous serons généreux avec le distingueur en lui procurant, à la fin de l'interaction, la clé K quand il interagit avec $(\mathsf{EMSP}_K^{\boldsymbol{P}}, \boldsymbol{P})$, ou une clé uniformément aléatoire K quand il interagit avec $(E, \boldsymbol{P})$. Cette considération se fait sans perte de généralité puisque le distingueur peut ignorer cette information. Ainsi, on peut voir maintenant une transcription τ comme un uplet $(\mathcal{Q}_E, \mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_m}, K)$. On appelle $(\mathcal{Q}_E, \mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_m})$ (sans la clé) la transcription des permutations, et on dit qu'une transcription τ est atteignable si la transcription des permutations correspondantes est atteignable. On note $\mathcal{T}$ l'ensemble des transcriptions atteignables. (Ainsi $\mathcal{T}$ dépend de $\mathcal{D}$ puisque la notion d'atteignable dépend de $\mathcal{D}$.) Par la suite, nous notons T_{re}, respectivement T_{id}, la distribution de probabilité d'une transcription τ induite par le monde réel, respectivement induite par le monde idéal (remarquons que ces deux distributions dépendent du distingueur). Par extension, on utilise les mêmes notations pour une variable aléatoire distribué selon l'une ou l'autre des deux distributions.

Théorème principal des coefficients H.

Afin de majorer l'avantage d'un distingueur, nous appliquerons toujours la même stratégie : nous partitionnerons l'ensemble des transcriptions atteignables en un ensemble de « bonnes » transcriptions $\mathcal{T}_1$ telles que la probabilité d'obtenir $\tau \in \mathcal{T}_1$ dans le monde réel est supérieure ou égale à une valeur proche de la probabilité d'obtenir τ dans le monde idéal, et un ensemble $\mathcal{T}_2$ de « mauvaises » transcriptions vérifiant la propriété inverse. Le théorème principal des coefficients H, ajusté aux notations précédentes, est :

Théorème 6.1 (Technique des Coefficients H). *Fixons un distingueur $\mathcal{D}$. Soit $\mathcal{T} = \mathcal{T}_1 \sqcup \mathcal{T}_2$ une partition de l'ensemble des transcriptions atteignables. Supposons qu'il existe ε_1 tel que, pour tout $\tau \in \mathcal{T}_1$, on a*[1]

$$\frac{\Pr[T_{\mathrm{re}} = \tau]}{\Pr[T_{\mathrm{id}} = \tau]} \geq 1 - \varepsilon_1 \,,$$

et qu'il existe ε_2 tel que

$$\Pr[T_{\mathrm{id}} \in \mathcal{T}_2] \leq \varepsilon_2 \,.$$

Alors $\mathbf{Adv}(\mathcal{D}) \leq \varepsilon_1 + \varepsilon_2$. ♢

Démonstration. La preuve est standard (voir [Pat91, Pat08]). Puisque la sortie du distingueur est une fonction déterministe de la transcription, l'avantage du distingueur est majoré par la distance statistique entre T_{id} et T_{re}, c'est-à-dire

$$\mathbf{Adv}(\mathcal{D}) \leq \|T_{\mathrm{re}} - T_{\mathrm{id}}\| \stackrel{\mathrm{def}}{=} \frac{1}{2} \sum_{\tau \in \mathcal{T}} |\Pr[T_{\mathrm{re}} = \tau] - \Pr[T_{\mathrm{id}} = \tau]| \,.$$

De plus, on a :

$$\begin{aligned}
\|T_{\mathrm{re}} - T_{\mathrm{id}}\| &= \sum_{\substack{\tau \in \mathcal{T} \\ \Pr[T_{\mathrm{id}}=\tau] > \Pr[T_{\mathrm{re}}=\tau]}} (\Pr[T_{\mathrm{id}} = \tau] - \Pr[T_{\mathrm{re}} = \tau]) \\
&= \sum_{\substack{\tau \in \mathcal{T} \\ \Pr[T_{\mathrm{id}}=\tau] > \Pr[T_{\mathrm{re}}=\tau]}} \Pr[T_{\mathrm{id}} = \tau] \left(1 - \frac{\Pr[T_{\mathrm{re}} = \tau]}{\Pr[T_{\mathrm{id}} = \tau]}\right) \\
&\leq \sum_{\tau \in \mathcal{T}_1} \Pr[T_{\mathrm{id}} = \tau]\varepsilon_1 + \sum_{\tau \in \mathcal{T}_2} \Pr[T_{\mathrm{id}} = \tau] \\
&\leq \varepsilon_1 + \varepsilon_2 \,.
\end{aligned}$$

■

Le rapport $\Pr[T_{\mathrm{re}} = \tau]/\Pr[T_{\mathrm{id}} = \tau]$ s'écrit d'une manière particulièrement simple pour le schéma d'Even-Mansour généralisé. (C'est l'une des raisons pour lesquelles on donne la clé K au distingueur à la fin de la transcription. Autrement, le rapport s'écrirait d'une manière bien plus complexe)

Lemme 6.2. *Soit $\tau = (\mathcal{Q}_E, \mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_m}, K) \in \mathcal{T}$ une transcription atteignable et on définit*

$$\mathsf{p}(\tau) \stackrel{\mathrm{def}}{=} \Pr\left[P_1, \ldots, P_m \leftarrow_{\$} \mathcal{P}_n : \mathsf{EMSP}_K^{P_1,\ldots,P_m} \vdash \mathcal{Q}_E \,\middle|\, (P_1 \vdash \mathcal{Q}_{P_1}) \wedge \cdots \wedge (P_m \vdash \mathcal{Q}_{P_m})\right] .$$

Alors

$$\frac{\Pr[T_{\mathrm{re}} = \tau]}{\Pr[T_{\mathrm{id}} = \tau]} = (N)_{q_e} \cdot \mathsf{p}(\tau) \,.$$ ▽

1. On rappelle que, pour toute transcription atteignable, on a $\Pr[T_{\mathrm{id}} = \tau] > 0$.

Démonstration. On vérifie facilement que l'interaction du distingueur avec n'importe quel ensemble de permutations $(P_0, P_1, \ldots, P_m)$ produit la transcription des permutations $(\mathcal{Q}_E, \mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_m})$ si et seulement si

$$(P_0 \vdash \mathcal{Q}_E) \wedge (P_1 \vdash \mathcal{Q}_{P_1}) \wedge \cdots \wedge (P_m \vdash \mathcal{Q}_{P_m}) .$$

Dans le monde idéal, la distingueur interagit avec $(P_0, P_1, \ldots, P_m)$ où P_0 est indépendante de $P_1, \ldots P_m$, et la clé K est uniformément aléatoire et indépendante des permutations. Ainsi

$$\Pr[T_{\mathrm{id}} = \tau] = \frac{1}{2^\ell} \times \frac{1}{(N)_{q_e}} \times \left(\frac{1}{(N)_{q_p}}\right)^m .$$

Dans le monde réel, le distingueur interagit avec $(\mathsf{EMSP}_K^{P_1,\ldots,P_m}, P_1, \ldots, P_m)$, où la clé K est uniformément aléatoire et indépendante de $(P_1, \ldots, P_m)$. Ainsi

$$\begin{aligned}\Pr[T_{\mathrm{re}} = \tau] = \frac{1}{2^\ell} \times \left(\frac{1}{(N)_{q_p}}\right)^m \\ \times \Pr\left[P_1, \ldots, P_m \leftarrow_{\$} \mathcal{P}_n : \mathsf{EMSP}_K^{P_1,\ldots,P_m} \vdash \mathcal{Q}_E \,\middle|\, (P_1 \vdash \mathcal{Q}_{P_1}) \wedge \cdots \wedge (P_m \vdash \mathcal{Q}_{P_m})\right] ,\end{aligned}$$

ce qui prouve le lemme. ∎

6.2.5 Lemmes utiles

Nous présentons dans cette section deux lemmes combinatoires qui seront très utiles par la suite pour nos preuves de sécurité.

Lemme 6.3. *Soient N, a, b, c, d des entiers positifs tels que $c + d = 2b$ et $2a + 2b \leq N$. Alors*

$$\frac{(N)_a (N-2b)_a}{(N-c)_a (N-d)_a} \geq 1 - \frac{4ab^2}{N^2} . \qquad \triangledown$$

Démonstration. Supposons, sans perte de généralité, que $c \geq d$. Cela implique que $c \geq b$ et

$$\begin{aligned}\frac{(N)_a (N-2b)_a}{(N-c)_a (N-d)_a} &= \frac{(N)_a (N-2b)_a}{((N-b)_a)^2} \times \frac{((N-b)_a)^2}{(N-c)_a (N-d)_a} \\ &= \prod_{i=N-a-b+1}^{N-b} \frac{(i+b)(i-b)}{i^2} \times \prod_{i=N-a-b+1}^{N-b} \frac{i^2}{(i-c+b)(i-d+b)} \\ &= \prod_{i=N-a-b+1}^{N-b} \left(1 - \frac{b^2}{i^2}\right) \times \underbrace{\prod_{i=N-a-b+1}^{N-b} \frac{i^2}{(i-(c-b))(i+(c-b))}}_{\geq 1} \\ &\geq \left(1 - \frac{b^2}{(N-a-b+1)^2}\right)^a \\ &\geq 1 - \frac{4ab^2}{N^2} ,\end{aligned}$$

où nous utilisons $a + b \leq N/2$ pour la dernière inégalité. ∎

Lemme 6.4. *Soient N, q des entiers positifs et $M > 0$. Supposons que $M \leq \frac{q}{2} \leq \frac{N}{6}$, et soit*

$$C_{N,q,k} = \frac{(q)_{2k}(N-2q)_{q-2k}(N)_q}{k!(N)_{2q-k}}\,.$$

Alors, on a

$$\sum_{0\leq k\leq M} C_{N,q,k} \geq 1 - \frac{2M^2}{q} - \frac{3q^2}{2MN}\,. \qquad \triangledown$$

Démonstration. Nous allons utiliser le fait que $C_{N,q,k}$ ressemble à une distribution hypergéométrique. Une distribution hypergéométrique est utilisée dans le cas d'un tirage sans remise dans un ensemble partitionné en deux sous-ensembles. On considère la variable aléatoire, paramétrée par N, p, et q, qui compte le nombre d'éléments dans le sous-ensemble des q « bons » éléments quand p éléments sont tirés, sans remise, dans l'univers des N éléments. La probabilité qu'exactement k éléments soient tirés dans l'ensemble des q bons éléments est

$$\mathsf{Hyp}_{N,p,q}(k) = \frac{\binom{q}{k}\binom{N-q}{p-k}}{\binom{N}{p}} = \frac{(p)_k(q)_k(N-q)_{p-k}}{k!(N)_p}\,,$$

et la moyenne de cette variable aléatoire est pq/N.

Pour $k \leq M$, on a

$$\begin{aligned}
C_{N,q,k} &= \frac{(q)_{2k}(N-2q)_{q-2k}(N)_q}{k!(N)_{2q-k}} \times \frac{k!(N-q)_q}{(q)_k(q)_k(N-2q)_{q-k}} \times \mathsf{Hyp}_{N-q,q,q}(k) \\
&= \frac{(q-k)_k}{(q)_k} \times \frac{(N-q)_q(N-2q)_{q-2k}}{(N-q)_{q-k}(N-2q)_{q-k}} \times \mathsf{Hyp}_{N-q,q,q}(k) \\
&= \prod_{i=0}^{k-1}\left(1-\frac{k}{q-i}\right) \times \underbrace{\frac{(N-2q+k)_k}{(N-3q+2k)_k}}_{\geq 1} \times \mathsf{Hyp}_{N-q,q,q}(k) \\
&\geq \left(1-\frac{k}{q-k+1}\right)^k \mathsf{Hyp}_{N-q,q,q}(k) \\
&\geq \left(1-\frac{k^2}{q-k+1}\right) \mathsf{Hyp}_{N-q,q,q}(k) \\
&\geq \left(1-\frac{2M^2}{q}\right) \mathsf{Hyp}_{N-q,q,q}(k)\,,
\end{aligned}$$

où la dernière inégalité vient du fait que $k \leq M \leq q/2$. Ainsi

$$\sum_{0\leq k\leq M} C_{N,q,k} \geq \left(1-\frac{2M^2}{q}\right) \sum_{0\leq k\leq M} \mathsf{Hyp}_{N-q,q,q}(k)\,.$$

Puisque la moyenne de la distribution hypergéométrique $\mathsf{Hyp}_{N-q,q,q}$ est $\frac{q^2}{N-q}$, on a

$$\sum_{k>M} \mathsf{Hyp}_{N-q,q,q}(k) \leq \frac{q^2}{M(N-q)} \leq \frac{3q^2}{2MN}$$

par l'inégalité de Markov et l'hypothèse que $q \leq N/3$. On en déduit que

$$\sum_{0\leq k\leq M} C_{N,q,k} \geq \left(1-\frac{2M^2}{q}\right) \sum_{0\leq k\leq M} \mathsf{Hyp}_{N-q,q,q}(k)$$
$$\geq \left(1-\frac{2M^2}{q}\right)\left(1-\frac{3q^2}{2MN}\right) \geq 1-\frac{2M^2}{q}-\frac{3q^2}{2MN}\,.$$

∎

6.3 Un théorème sur le sum-capture problem

Dans cette section, nous prouvons une variante d'un résultat précédent sur le « sum-capture problem » [Bab89, KPS13, Ste13]. Ce résultat prouve que, lorsqu'on choisit un sous-ensemble aléatoire A de $\mathbb{Z}_2^n$ (et plus généralement n'importe quel groupe abélien) de taille q, la valeur

$$\mu(A) = \max_{\substack{U,V\subseteq\mathbb{Z}_2^n \\ |U|=|V|=q}} |\{(a,u,v)\in A\times U\times V : a = u\oplus v\}|$$

est proche de son espérance q^3/N (si A, U et V étaient uniformément aléatoires) avec une probabilité très proche de 1. Ici, nous prouvons un résultat de ce type dans le cadre où A est construit à partir de l'interaction d'un distingueur avec une permutation aléatoire P, à savoir $A = \{x\oplus y : (x,y)\in\mathcal{Q}\}$, où $\mathcal{Q}$ est la transcription de l'interaction entre le distingueur et P. En fait, notre résultat est même plus général car le cas particulier que nous venons d'évoquer correspond au cas où Γ est l'identité dans le théorème suivant.

Théorème 6.5. *Fixons un automorphisme $\Gamma \in \mathsf{GL}(n)$. Soit P une permutation uniformément aléatoire de $\{0,1\}^n$, et soit $\mathcal{A}$ un algorithme probabiliste faisant exactement q requêtes adaptatives (directes ou inverses) à P. Soit $\mathcal{Q} = ((x_1,y_1),\ldots,(x_q,y_q))$ la transcription de l'interaction entre $\mathcal{A}$ et P. Pour tous sous-ensembles U et V de $\{0,1\}^n$, soit*

$$\mu(\mathcal{Q},U,V) = |\{((x,y),u,v)\in\mathcal{Q}\times U\times V : x\oplus u = \Gamma(y\oplus v)\}|\,.$$

Alors, en supposant que $9n \leq q \leq N/2$, on a

$$\Pr_{P,\omega}\left[\exists U,V\subseteq\{0,1\}^n : \mu(\mathcal{Q},U,V) \geq \frac{q|U||V|}{N} + \frac{2q^2\sqrt{|U||V|}}{N} + 3\sqrt{nq|U||V|}\right] \leq \frac{2}{N}\,,$$

où la probabilité est prise sur le choix aléatoire de P et l'aléa ω de $\mathcal{A}$. ♢

Démonstration. Le théorème se déduit directement des lemmes 6.6 et 6.8 que nous prouvons ci-dessous. ∎

Rappels sur l'analyse de Fourier

Nous commençons par introduire quelques notations et quelques résultats classiques sur l'analyse de Fourier sur le groupe abélien $\mathbb{Z}_2^n$. Étant donné un sous-ensemble $S\subset\{0,1\}^n$, on note $1_S : \{0,1\}^n \to \{0,1\}$ la fonction caractérique de S, c'est-à-dire la fonction définie par

$1_S(x) = 1$ si $x \in S$ et $1_S(x) = 0$ si $x \notin S$. Étant données deux fonctions $f, g : \{0,1\}^n \to \mathbb{R}$, on note

$$\langle f, g \rangle = \mathbb{E}[fg] = \frac{1}{N} \sum_{x \in \{0,1\}^n} f(x)g(x)$$

le produit scalaire de f et g, et, pour tout $x \in \{0,1\}^n$, on note

$$(f * g)(x) = \sum_{y \in \{0,1\}^n} f(y)g(x \oplus y)$$

la convolution de f et g. Etant donné $\alpha \in \{0,1\}^n$, on note $\chi_\alpha : \{0,1\}^n \to \{\pm 1\}$ le *caractère* associé à α défini par

$$\chi_\alpha(x) = (-1)^{\alpha \cdot x}\,.$$

Le caractère trivial χ_0 est appelé le *caractère principal*. Tous les autres caractères $\chi \neq 1$ correspondant à $\alpha \neq 0$ sont appelés *caractères non-principaux*. L'ensemble de tous les caractères forme un groupe pour l'opération $(\chi_\alpha \chi_\beta)(x) = \chi_\alpha(x)\chi_\beta(x)$ et on a $\chi_\alpha \chi_\beta = \chi_{\alpha \oplus \beta}$.

Étant donnée une fonction $f : \{0,1\}^n \to \mathbb{R}$ et $\alpha \in \{0,1\}^n$, le *coefficient de Fourier* de f correspondant à α est

$$\widehat{f}(\alpha) \stackrel{\text{def}}{=} \langle f, \chi_\alpha \rangle = \frac{1}{N} \sum_{x \in \{0,1\}^n} f(x)(-1)^{\alpha \cdot x}\,.$$

Le coefficient correspondant à $\alpha = 0$ est appelé le *coefficient de Fourier principal*, tous les autres sont appelés *coefficients de Fourier non-principaux*. Remarquons que, pour un ensemble $S \subseteq \{0,1\}^n$, on a

$$\widehat{1_S}(0) = \frac{|S|}{N}\,,$$

c'est-à-dire que le coefficient de Fourier principal de 1_S est égal à la taille relative de l'ensemble S. Nous allons également utiliser les trois résultats classiques suivants, valables pour toutes fonctions $f, g, : \{0,1\}^n \to \mathbb{R}$, tout $\alpha \in \{0,1\}^n$, et tout $S \subseteq \{0,1\}^n$:

$$\sum_{x \in \{0,1\}^n} f(x)g(x) = N \sum_{\alpha \in \{0,1\}^n} \widehat{f}(\alpha)\widehat{g}(\alpha) \tag{6.3}$$

$$\widehat{(f * g)}(\alpha) = N\widehat{f}(\alpha)\widehat{g}(\alpha) \tag{6.4}$$

$$\sum_{\alpha \in \{0,1\}^n} |\widehat{1_S}(\alpha)|^2 = \frac{|S|}{N}\,. \tag{6.5}$$

Première étape : l'inégalité de Cauchy-Schwarz.

Avant de prouver le théorème 6.5, nous commençons par majorer $\mu(\mathcal{Q}, U, V)$ en terme d'amplitude maximale de coefficients de Fourier non-principaux de la fonction caractéristique $\widehat{1_\mathcal{Q}}$ de l'ensemble $\mathcal{Q} = ((x_1, y_1), \ldots, (x_q, y_q))$, vu comme un sous-ensemble de $\{0,1\}^{2n}$. Cette partie est adaptée de Babai [Bab89, Section 4] et Steinberger [Ste13], mais dans notre cas, nous travaillons sur le groupe produit $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$ (en particulier, le lemme 6.6 ci-dessous est l'analogue du théorème 4.1 de [Bab89], qui fut redécouvert de manière indépendante

par Steinberger [Ste13]). Notons, pour tout $\alpha \in \{0,1\}^n$, $\alpha \neq 0$,

$$\Phi_{\alpha,\Gamma}(\mathcal{Q}) \stackrel{\text{def}}{=} N^2 \left|\widehat{1_{\mathcal{Q}}}(\alpha, \Gamma^*(\alpha))\right| = \left|\sum_{(x,y)\in\mathcal{Q}} (-1)^{\alpha\cdot x \oplus \Gamma^*(\alpha)\cdot y}\right|$$
$$\Phi_{\Gamma}(\mathcal{Q}) \stackrel{\text{def}}{=} \max_{\alpha\neq 0} \Phi_{\alpha,\Gamma}(\mathcal{Q})\,.$$

Lemme 6.6. *Pour tous sous-ensembles U et V de $\{0,1\}^n$, on a*

$$\mu(\mathcal{Q}, U, V) \leq \frac{q|U||V|}{N} + \Phi_\Gamma(\mathcal{Q})\sqrt{|U||V|}\,. \qquad \triangledown$$

Démonstration. Notons

$$W = U \times V = \{(u,v) : u \in U, v \in V\}$$
$$K = \{(\Gamma(k), k) : k \in \{0,1\}^n\}\,.$$

Puisque $((x,y),u,v) \in \mathcal{Q}\times U \times V$ vérifie $x \oplus u = \Gamma(y \oplus v)$ si et seulement si il existe $k \in \{0,1\}^n$ tel que

$$(x,y) \oplus (u,v) = (\Gamma(k), k)\,,$$

on en déduit que

$$\begin{aligned}
\mu(\mathcal{Q},U,V) &= \sum_{\substack{(x,y)\in(\{0,1\}^n)^2\\(u,v)\in(\{0,1\}^n)^2}} 1_{\mathcal{Q}}(x,y)1_W(u,v)1_K(x\oplus u, y\oplus v)\\
&= \sum_{(x,y)\in(\{0,1\}^n)^2} 1_{\mathcal{Q}}(x,y) \sum_{(u,v)\in(\{0,1\}^n)^2} 1_W(u,v)1_K(x\oplus u, y\oplus v)\\
&= \sum_{(x,y)\in(\{0,1\}^n)^2} 1_{\mathcal{Q}}(x,y)(1_W * 1_K)(x,y)\\
&= N^2 \sum_{(\alpha,\beta)\in(\{0,1\}^n)^2} \widehat{1_{\mathcal{Q}}}(\alpha,\beta)\widehat{(1_W * 1_K)}(\alpha,\beta) \qquad \text{(par (6.3))}\\
&= N^4 \sum_{(\alpha,\beta)\in(\{0,1\}^n)^2} \widehat{1_{\mathcal{Q}}}(\alpha,\beta)\widehat{1_W}(\alpha,\beta)\widehat{1_K}(\alpha,\beta) \qquad \text{(par (6.4))}\,.
\end{aligned}$$

En séparant le coefficient de Fourier principal, on a

$$\begin{aligned}
\mu(\mathcal{Q},U,V) &= N^4\frac{|\mathcal{Q}|}{N^2}\frac{|W|}{N^2}\frac{|K|}{N^2} + N^4 \sum_{(\alpha,\beta)\neq(0,0)} \widehat{1_{\mathcal{Q}}}(\alpha,\beta)\widehat{1_W}(\alpha,\beta)\widehat{1_K}(\alpha,\beta)\\
&= \frac{q|U||V|}{N} + N^4 \sum_{(\alpha,\beta)\neq(0,0)} \widehat{1_{\mathcal{Q}}}(\alpha,\beta)\widehat{1_W}(\alpha,\beta)\widehat{1_K}(\alpha,\beta)\,. \qquad (6.6)
\end{aligned}$$

(Remarquons que l'égalité (6.6) ci-dessus est en fait vraie pour tout groupe abélien G et toute permutation $\Gamma : G \to G$ fixée, non-nécessairement linéaire, en remplaçant la somme sur les $(\alpha,\beta) \neq (0,0)$ par la somme sur les caractères non-principaux du groupe produit

$G \times G$.) De plus, on a

$$\begin{aligned}
\widehat{1_W}(\alpha,\beta) &= \frac{1}{N^2} \sum_{(u,v)\in(\{0,1\}^n)^2} 1_W(u,v)(-1)^{\alpha\cdot u\oplus\beta\cdot v} \\
&= \frac{1}{N^2} \sum_{(u,v)\in(\{0,1\}^n)^2} 1_U(u)1_V(v)(-1)^{\alpha\cdot u\oplus\beta\cdot v} \\
&= \frac{1}{N^2} \left(\sum_{u\in\{0,1\}^n} 1_U(u)(-1)^{\alpha\cdot u} \right) \left(\sum_{v\in\{0,1\}^n} 1_V(v)(-1)^{\beta\cdot v} \right) \\
&= \widehat{1_U}(\alpha)\widehat{1_V}(\beta)\,,
\end{aligned}$$

et

$$\begin{aligned}
\widehat{1_K}(\alpha,\beta) &= \frac{1}{N^2} \sum_{(x,y)\in(\{0,1\}^n)^2} 1_K(x,y)(-1)^{\alpha\cdot x\oplus\beta\cdot y} \\
&= \frac{1}{N^2} \sum_{y\in\{0,1\}^n} (-1)^{\alpha\cdot\Gamma(y)\oplus\beta\cdot y} \\
&= \frac{1}{N^2} \sum_{y\in\{0,1\}^n} (-1)^{\Gamma^*(\alpha)\cdot y\oplus\beta\cdot y} \\
&= 0 \text{ if } \beta \neq \Gamma^*(\alpha) \\
&\quad \frac{1}{N} \text{ if } \beta = \Gamma^*(\alpha)\,.
\end{aligned}$$

Et alors, en injectant les deux équations précédentes dans (6.6), on obtient

$$\begin{aligned}
\mu(\mathcal{Q},U,V) &= \frac{q|U||V|}{N} + N^3 \sum_{\alpha\neq 0} \widehat{1_{\mathcal{Q}}}(\alpha,\Gamma^*(\alpha))\widehat{1_U}(\alpha)\widehat{1_V}(\Gamma^*(\alpha)) \\
&\leq \frac{q|U||V|}{N} + N^3 \sum_{\alpha\neq 0} \left|\widehat{1_{\mathcal{Q}}}(\alpha,\Gamma^*(\alpha))\right| \cdot \left|\widehat{1_U}(\alpha)\right| \cdot \left|\widehat{1_V}(\Gamma^*(\alpha))\right| \\
&\leq \frac{q|U||V|}{N} + N\Phi_\Gamma(\mathcal{Q}) \sum_{\alpha\neq 0} \left|\widehat{1_U}(\alpha)\right| \cdot \left|\widehat{1_V}(\Gamma^*(\alpha))\right|\,,
\end{aligned}$$

où la dernière inégalité vient du fait que $|\widehat{1_{\mathcal{Q}}}(\alpha,\Gamma^*(\alpha))| \leq \Phi_\Gamma(\mathcal{Q})/N^2$ pour tout $\alpha \neq 0$ (par définition de $\Phi_\Gamma(\mathcal{Q})$). Par Cauchy-Schwarz,

$$\sum_{\alpha\neq 0} \left|\widehat{1_U}(\alpha)\right| \cdot \left|\widehat{1_V}(\Gamma^*(\alpha))\right| \leq \sqrt{\sum_{\alpha\in\{0,1\}^n} |\widehat{1_U}(\alpha)|^2} \sqrt{\sum_{\alpha\in\{0,1\}^n} |\widehat{1_V}(\Gamma^*(\alpha))|^2} = \frac{1}{N}\sqrt{|U||V|}\,,$$

où la dernière égalité vient de (6.5), et donc

$$\mu(\mathcal{Q},U,V) \leq \frac{q|U||V|}{N} + \Phi_\Gamma(\mathcal{Q})\sqrt{|U||V|}\,. \qquad \blacksquare$$

Majoration des coefficients de Fourier non-principaux

Ayant prouvé le lemme 6.6, il reste à trouver une majoration sur $\Phi_\Gamma(\mathcal{Q})$ qui soit vraie avec une forte probabilité sur les choix aléatoires de P et l'aléa de l'adversaire. Pour cela, nous avons besoin de l'extension suivante de la borne de Chernoff pour des variables aléatoires « modérément dépendantes ».

Lemme 6.7. *Soit $0 \leq \varepsilon \leq 1/2$, et $\boldsymbol{A} = (A_i)_{1\leq i\leq q}$ une suite de variables aléatoires à valeurs dans $\{\pm 1\}$. Supposons que, pour tout $1 \leq i \leq q$ et toute suite $(a_1, \ldots, a_{i-1}) \in \{\pm 1\}^{i-1}$, on a*

$$\Pr\left[A_i = 1 \,|\, (A_1, \ldots, A_{i-1}) = (a_1, \ldots a_{i-1})\right] \leq \frac{1}{2} + \varepsilon\,.$$

Alors, pour tout $\delta \in [0, 1]$, on a

$$\Pr\left[\sum_{i=1}^{q} A_i \geq q(2\varepsilon + \delta)\right] \leq e^{-\frac{q\delta^2}{12}}\,. \qquad \triangledown$$

Démonstration. Soit $\boldsymbol{B} = (B_i)_{1\leq i\leq q}$ des variables aléatoires indépendantes et identiquement distribuées telles que

$$\Pr[B_i = 1] = \frac{1}{2} + \varepsilon \quad \text{et} \quad \Pr[B_i = -1] = \frac{1}{2} - \varepsilon\,.$$

Nous montrons que, pour tout r, on a

$$\Pr\left[\sum_{i=1}^{q} A_i \geq r\right] \leq \Pr\left[\sum_{i=1}^{q} B_i \geq r\right]\,. \tag{6.7}$$

Nous prouvons cette équation à l'aide d'un coupling. Soit Ber_p la distribution de Bernouilli de paramètre p à valeurs dans ± 1 (c'est-à-dire que Ber_p vaut 1 avec probabilité p et -1 avec probabilité $1 - p$). Considérons l'échantillonnage suivant (on suppose que $\varepsilon < 1/2$, sans perte de généralité puisque le lemme est trivial pour $\varepsilon = 1/2$) :

for $i = 1$ to q **do**
  $p \leftarrow \Pr\left[A_i = 1 \,|\, (A_1, \ldots, A_{i-1}) = (u_1, \ldots u_{i-1})\right]$
  $u_i \leftarrow \mathsf{Ber}_p$
  if $u_i = 1$ **then**
    $v_i \leftarrow 1$
  else
    $p' \leftarrow \frac{1/2+\varepsilon-p}{1-p}$
    $v_i \leftarrow \mathsf{Ber}_{p'}$
return $((u_1, \ldots, u_q), (v_1, \ldots, v_q))$

Alors, clairement, $(u_1, \ldots, u_q) \sim \boldsymbol{A}$. De plus, $(v_1, \ldots, v_q) \sim \boldsymbol{B}$. En effet, pour tout $i = 1, \ldots, q$, et toute suite $(v_1, \ldots, v_{i-1}) \in \{\pm 1\}^{i-1}$, on a

$$\Pr[v_i = 1 | (v_1, \ldots, v_{i-1})] = p + p'(1 - p) = \frac{1}{2} + \varepsilon\,.$$

Remarquons que, durant l'échantillonage, $u_i = 1$ implique que $v_i = 1$, et donc, pour tout r,

$$\sum_{i=1}^{q} u_i \geq r \Longrightarrow \sum_{i=1}^{q} v_i \geq r\,,$$

ce qui prouve (6.7).

Fixons maintenant $\delta \in [0,1]$, et soit $(B'_i)_{1\le i\le q}$ défini par

$$B'_i = \frac{1+B_i}{2}\,,$$

alors

$$\Pr[B'_i = 1] = \frac{1}{2} + \varepsilon \quad \text{et} \quad \Pr[B'_i = 0] = \frac{1}{2} - \varepsilon\,.$$

Soit $m = \mathbb{E}(\sum_{i=1}^{q} B'_i) = q(1/2+\varepsilon)$. On sait que la borne de Chernoff établit que, pour tout $0 \le \delta' \le 1$, on a

$$\Pr\left[\sum_{i=1}^{q} B'_i \ge (1+\delta')m\right] \le e^{\frac{-m\delta'^2}{3}}\,.$$

En remplaçant alors δ' par $\frac{q\delta}{2m} = \frac{\delta}{1+2\varepsilon}$ dans l'inégalité précédente, on obtient (remarquons que $\delta \in [0,1] \Rightarrow \delta' \in [0,1]$)

$$\Pr\left[\sum_{i=1}^{q} B_i \ge q(2\varepsilon+\delta)\right] = \Pr\left[\sum_{i=1}^{q} B'_i \ge \left(1+\frac{q\delta}{2m}\right)m\right] \le e^{-\frac{q^2\delta^2}{12m}} \le e^{-\frac{q\delta^2}{12}}\,.$$

qui, combiné à (6.7), permet de conclure. ∎

Nous sommes maintenant prêts pour prouver une majoration intéressante sur $\Phi_\Gamma(\mathcal{Q})$.

Lemme 6.8. *Supposons que $9n \le q \le N/2$. Fixons $\Gamma \in \mathsf{GL}(n)$ et un attaquant $\mathcal{A}$ faisant q requêtes à une permutation aléatoire P. Soit $\mathcal{Q}$ la transcription de l'interaction de $\mathcal{A}$ avec P. Alors*

$$\Pr_{P,\omega}\left[\Phi_\Gamma(\mathcal{Q}) \ge \frac{2q^2}{N} + 3\sqrt{nq}\right] \le \frac{2}{N}\,,$$

où la probabilité est prise sur l'aléa de P et l'aléa ω de $\mathcal{A}$. ▽

Démonstration. Dans toute cette preuve, $\Pr[\cdot]$ correspond à $\Pr_{P,\omega}[\cdot]$. Fixons $\alpha \in \{0,1\}^n$, $\alpha \ne 0$. Soit $\mathcal{Q} = ((x_1,y_1),\dots,(x_q,y_q))$ suivant l'ordre naturel des requêtes de $\mathcal{A}$, on définit la suite de variables aléatoires $(A_i)_{1\le i\le q}$ où $A_i = (-1)^{\alpha.x_i \oplus \Gamma^*(\alpha)\cdot y_i}$. Alors $\Phi_{\alpha,\Gamma}(\mathcal{Q}) = |\sum_{i=1}^{q} A_i|$. Pour utiliser le lemme 6.7, nous allons montrer que, pour tout $1 \le i \le q$ et toute suite $\boldsymbol{a} = (a_1,\dots,a_{i-1}) \in \{\pm 1\}^{i-1}$, on a

$$p_i \stackrel{\text{def}}{=} \Pr\left[A_i = 1 \,|\, (A_1,\dots,A_{i-1}) = (a_1,\dots,a_{i-1})\right] \le \frac{1}{2} + \frac{q}{N}\,. \tag{6.8}$$

Soit $\mathcal{Q}_i = ((x_1,y_1),\dots,(x_i,y_i))$ les i premières paires de la transcription $\mathcal{Q}$ et $\Theta_{\boldsymbol{a}}$ l'ensemble des transcriptions partielles atteignables $\mathcal{Q}_{i-1}$ telles que $(A_1,\dots,A_{i-1}) = (a_1,\dots,a_{i-1})$. Alors

$$\begin{aligned}
p_i &= \frac{\Pr\left[A_i = 1 \wedge (A_1,\dots,A_{i-1}) = (a_1,\dots,a_{i-1})\right]}{\Pr[(A_1,\dots,A_{i-1}) = (a_1,\dots,a_{i-1})]} \\
&= \frac{\sum_{(x'_j,y'_j)_{1\le j\le i-1}\in\Theta_{\boldsymbol{a}}} \Pr\left[A_i = 1 \wedge \mathcal{Q}_{i-1} = (x'_j,y'_j)_{1\le j\le i-1}\right]}{\sum_{(x'_j,y'_j)_{1\le j\le i-1}\in\Theta_{\boldsymbol{a}}} \Pr[\mathcal{Q}_{i-1} = (x'_j,y'_j)_{1\le j\le i-1}]} \\
&= \frac{\sum_{(x'_j,y'_j)_{1\le j\le i-1}\in\Theta_{\boldsymbol{a}}} \Pr\left[A_i = 1 \middle| \mathcal{Q}_{i-1} = (x'_j,y'_j)_{1\le j\le i-1}\right] \Pr\left[\mathcal{Q}_{i-1} = (x'_j,y'_j)_{1\le j\le i-1}\right]}{\sum_{(x'_j,y'_j)_{1\le j\le i-1}\in\Theta_{\boldsymbol{a}}} \Pr\left[\mathcal{Q}_{i-1} = (x'_j,y'_j)_{1\le j\le i-1}\right]}\,.
\end{aligned} \tag{6.9}$$

Fixons maintenant une transcription partielle arbitraire $((x'_1, y'_1), \ldots, (x'_{i-1}, y'_{i-1}))$. Supposons que la i-ème requête de l'adversaire à P est la requête directe x_i. Remarquons que la réponse y_i est uniformément aléatoire dans un ensemble de taille $N-i+1$. Remarquons également que, une fois qu'x_i est fixé, il y a exactement $N/2$ y_i tels que $(-1)^{\alpha.x_i \oplus \Gamma^*(\alpha)\cdot y_i} = 1$ puisque $\Gamma^*(\alpha)$ est non-nul. De la même manière, si la i-ème requête est une requête inverse y_i, alors la réponse x_i est uniformément aléatoire dans un ensemble de taille $N-i+1$, et une fois qu'y_i est fixé, il y a exactement $N/2$ x_i tels que $(-1)^{\alpha.x_i \oplus \Gamma^*(\alpha)\cdot y_i} = 1$ puisque $\alpha \neq 0$. Ainsi, on a

$$\begin{aligned}\Pr\left[A_i = 1 \middle| \mathcal{Q}_{i-1} = ((x'_1, y'_1), \ldots, (x'_{i-1}, y'_{i-1}))\right] &\leq \frac{N/2}{N-i+1} \\ &\leq \frac{N}{2(N-q)} \leq \frac{1}{2} + \frac{q}{2(N-q)} \leq \frac{1}{2} + \frac{q}{N}\,,\end{aligned}$$

ce qui implique que la même borne est vraie pour p_i par (6.9), prouvant ainsi (6.8). On peut maintenant utiliser le lemme 6.7 avec $\varepsilon = q/N$ et on a, pour tout $\delta \in [0,1]$,

$$\Pr\left[\sum_{i=1}^{q} A_i \geq \frac{2q^2}{N} + q\delta\right] \leq e^{-\frac{q\delta^2}{12}}\,.$$

En posant $A'_i = -A_i$ et en appliquant exactement le même raisonnement, on a

$$\Pr\left[\sum_{i=1}^{q} A_i \leq -\left(\frac{2q^2}{N} + q\delta\right)\right] \leq e^{-\frac{q\delta^2}{12}}\,.$$

Et donc

$$\Pr\left[\Phi_{\alpha,\Gamma}(\mathcal{Q}) \geq \frac{2q^2}{N} + q\delta\right] \leq 2e^{-\frac{q\delta^2}{12}}\,.$$

Puisque cette inégalité est vraie pour tout $\alpha \neq 0$, en choisissant $\delta = \sqrt{(12\ln N)/q}$ (ce qui, en supposant que $q \geq 9n$, implique que $\delta \leq 1$), on obtient finalement, en utilisant $\sqrt{12\ln 2} \leq 3$,

$$\Pr_{P,\omega}\left[\Phi_\Gamma(\mathcal{Q}) \geq \frac{2q^2}{N} + 3\sqrt{nq}\right] \leq \frac{2}{N}\,.$$

■

6.4 Slide Attacks contre certaines versions du schéma d'Even-Mansour généralisé

Nous présentons dans cette section différentes attaques, appelées « slide attacks » [BW99, BW00], face aux cas particuliers du schéma à r tours avec clés et permutations identiques puis du cas où les clés ne sont pas forcément identiques mais diffèrent d'une constante.

6.4.1 Slide Attack dans le cas de clés identiques et de permutations identiques

Considérons le schéma d'Even-Mansour à r tours avec une seule permutation P et une seule clé k, qu'on notera simplement EMSP_k^P ici. Nous allons présenter une « slide attack » contre ce schéma avec une complexité en requête et en temps de calcul de $\mathcal{O}(2^{n/2})$,

indépendamment du nombre de tours r. Décrivons l'attaque d'un adversaire $\mathcal{D}$ interagissant avec une paire de permutations (E, P), et devant distinguer si E est uniformément aléatoire ou si E est de la forme EMSP_k^P pour une clé aléatoire k :

1. Fixons $c \in \{0,1\}^n$ non-nul et deux sous-ensembles X, $U \subset \{0,1\}^n$ tels que $|X| = |U| = 2^{\frac{n}{2}}$ et
$$X \oplus U = \{x \oplus u : x \in X, u \in U\} = \{0,1\}^n.$$
(Par exemple, X correspond à toutes les chaînes dont les $n/2$ derniers bits sont nuls, et U les chaînes dont les $n/2$ premiers bits sont nuls.)
2. $\mathcal{D}$ fait les requêtes
   - $E(x)$ et $E(x \oplus c)$ pour $x \in X$
   - $P(u)$ et $P(u \oplus c)$ pour $u \in U$
3. En utilisant les réponses des requêtes précédentes, $\mathcal{D}$ fait les requêtes
   - $E(P(u))$ et $E(P(u \oplus c))$ pour $u \in U$
   - $P(E(x))$ et $P(E(x \oplus c))$ pour $x \in X$
4. Si il existe $x^* \in X$ et $u^* \in U$ tels que
$$P(E(x^*)) \oplus E(P(u^*)) = P(E(x^* \oplus c)) \oplus E(P(u^* \oplus c)) = x^* \oplus u^* \tag{6.10}$$
alors $\mathcal{D}$ répond 1. Sinon, $\mathcal{D}$ répond 0.

Les nombres de requêtes à E et de requêtes à P pour cette attaque sont tous les deux majorés par $2^{2+\frac{n}{2}}$ (il peut y avoir des requêtes redondantes). De plus, cette attaque peut facilement être transformée en attaque pour récupérer la clé k, l'adversaire tentant la clé $k = x^* \oplus u^*$ pour (x^*, u^*) vérifiant l'équation (6.10).

Analysons la probabilité de succès de cette attaque. Quand $\mathcal{D}$ interagit avec le monde réel (EMSP_k^P, P), il répond toujours 1 puisque la paire (x^*, u^*) vérifiant $x^* \oplus u^* = k$, où k est la clé secrète, vérifie nécessairement l'équation (6.10). Cela peut facilement être vu à partir de la propriété de « commutativité » suivante, vraie pour tout $x \in \{0,1\}^n$:

$$k \oplus P(\mathsf{EMSP}_k^P(x)) = \mathsf{EMSP}_k^P(P(k \oplus x)).$$

Quand $\mathcal{D}$ interagit avec le monde idéal (E, P), nous allons montrer que la probabilité de trouver (x^*, u^*) vérifiant (6.10) est faible. Fixons une paire arbitaire $(x, u) \in X \times U$. Pour tout uplet (y, y', v, v') de chaînes de n bits telles que $y \neq y'$ et $v \neq v'$, on définit

$$\begin{aligned}\mathsf{p}(y, y', v, v') &\stackrel{\text{def}}{=} \Pr\left[(x,u) \text{ vérifie (6.10)} \;\middle|\; \begin{array}{l} E(x) = y \wedge E(x \oplus c) = y' \\ P(u) = v \wedge P(u \oplus c) = v' \end{array}\right] \\ &= \Pr\left[P(y) \oplus E(v) = P(y') \oplus E(v') = x \oplus u \;\middle|\; \begin{array}{l} E(x) = y \wedge E(x \oplus c) = y' \\ P(u) = v \wedge P(u \oplus c) = v' \end{array}\right].\end{aligned}$$

Afin de majorer $\mathsf{p}(y, y', v, v')$, on distingue les quatres cas suivants :

1. Si ($y \notin \{u, u \oplus c\}$ ou $v \notin \{x, x \oplus c\}$) et ($y' \notin \{u, u \oplus c\}$ ou $v' \notin \{x, x \oplus c\}$), alors
$$\mathsf{p}(y, y', v, v') \leq \frac{1}{(N-2)(N-3)}.$$
2. Si ($y \in \{u, u \oplus c\}$ et $v \in \{x, x \oplus c\}$) et ($y' \notin \{u, u \oplus c\}$ ou $v' \notin \{x, x \oplus c\}$), alors
$$\mathsf{p}(y, y', v, v') \leq \frac{1}{(N-2)}.$$

3. Si $(y \notin \{u, u \oplus c\}$ ou $v \notin \{x, x \oplus c\})$ et $(y' \in \{u, u \oplus c\}$ et $v' \in \{x, x \oplus c\})$, alors
$$\mathsf{p}(y, y', v, v') \leq \frac{1}{(N-2)}.$$
4. Si $y \in \{u, u \oplus c\}$, $v \in \{x, x \oplus c\}$, $y' \in \{u, u \oplus c\}$, et $v' \in \{x, x \oplus c\}$, alors
$$\mathsf{p}(y, y', v, v') \leq 1.$$

Il reste à majorer le nombre d'uplets (y, y', v, v') pour chaque cas, et on obtient :

$$\begin{aligned}
\Pr\left[(x,u) \text{ vérifie (6.10)}\right] &\leq \frac{1}{N^2(N-1)^2} \sum_{(y,y',v,v')} \mathsf{p}(y, y', v, v') \\
&\leq \frac{1}{N^2(N-1)^2} \left(\underbrace{\frac{N^2(N-1)^2}{(N-2)(N-3)}}_{\text{cas 1}} + 2 \cdot \underbrace{\frac{4(N-1)^2}{N-2}}_{\text{cas 2\&3}} + \underbrace{4}_{\text{cas 4}} \right) \\
&\leq \frac{1}{(N-2)(N-3)} + \frac{8}{N^2(N-2)} + \frac{4}{N^2(N-1)^2}.
\end{aligned}$$

En sommant sur les $(x, u) \in X \times U$, on a finalement

$$\Pr[\exists (x,u) \text{ vérifiant (6.10)}] \leq \frac{N}{(N-2)(N-3)} + \frac{8}{N(N-2)} + \frac{4}{N(N-1)^2} = \mathcal{O}\left(\frac{1}{N}\right).$$

Ainsi, quand $\mathcal{D}$ interagit avec le monde idéal, il répond 1 avec une probabilité proche de 0 quand N est grand. Ce qui prouve le lemme suivant.

Théorème 6.9. *Considérons le schéma d'Even-Mansour généralisé à r tours avec une seule permutation et une seule clé* $\mathsf{EMSP}[n, r, \ell = n, \boldsymbol{\gamma} = \mathbf{Id}]$. *Alors il existe une attaque qui permet de distinguer ce schéma d'une permutation aléatoire en faisant, au plus,* $2^{2+\frac{n}{2}}$ *requêtes à la permutation externe et à la permutation interne, et dont l'avantage est* $1 - \mathcal{O}(\frac{1}{N})$. ♢

6.4.2 Extension au cas des clés de tours xorées par des constantes

Nous montrons dans cette section que l'attaque présentée dans la section précédente peut être étendue au schéma d'Even-Mansour généralisé à deux tours et une permutation où les clés de tours sont de la forme $k_i = k \oplus t_i$, où k est la clé principale de n bits et (t_0, t_1, t_2) est un uplet (publique) de trois constantes de n bits. Le distingueur, interagissant avec une paire de permutations (E, P), procède de la manière suivante :

1. Il fixe $c \in \{0,1\}^n$ non-nul et deux sous-ensembles X, $U \subset \{0,1\}^n$ tels que $|X| = |U| = 2^{\frac{n}{2}}$ et
$$X \oplus U = \{x \oplus u : x \in X, u \in U\} = \{0,1\}^n.$$
(Par exemple, X peut être l'ensemble des chaînes de n bits dont les $n/2$ derniers bits sont nuls, et U l'ensemble des chaînes de n bits dont les $n/2$ premiers bits sont nuls.)
2. $\mathcal{D}$ fait les requêtes
   – $E(x)$ et $E(x \oplus c)$ pour $x \in X$

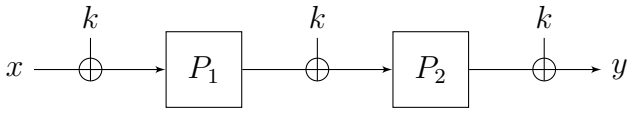

FIGURE 6.3 – Le schéma d'Even-Mansour généralisé à 2 tours avec des permutations indépendantes et des clés de tours identiques.

- $P(u)$ et $P(u \oplus c)$ pour $u \in U$

3. En utilisant les réponses des requêtes précédentes, $\mathcal{D}$ fait les requêtes
   - $E(t_0 \oplus t_1 \oplus P(u))$ et $E(t_0 \oplus t_1 \oplus P(u \oplus c))$ pour $u \in U$
   - $P(t_1 \oplus t_2 \oplus E(x))$ et $P(t_1 \oplus t_2 \oplus E(x \oplus c))$ pour $x \in X$
4. Si il existe $x^* \in X$ et $u^* \in U$ tels que

$$\begin{cases} P(t_1 \oplus t_2 \oplus E(x^*)) \oplus E(t_0 \oplus t_1 \oplus P(u^*)) = t_0 \oplus t_2 \oplus x^* \oplus u^* \\ P(t_1 \oplus t_2 \oplus E(x^* \oplus c)) \oplus E(t_0 \oplus t_1 \oplus P(u^* \oplus c)) = t_0 \oplus t_2 \oplus x^* \oplus u^* \end{cases} \tag{6.11}$$

   alors $\mathcal{D}$ répond 1. Sinon, $\mathcal{D}$ répond 0.

Le nombre de requêtes à E et le nombre de requêtes à P sont tous les deux d'au plus $2^{2+\frac{n}{2}}$ (il peut y avoir des requêtes redondantes). De plus, cette attaque peut facilement être utilisée pour retrouver la clé k en tentant les clés $k = t_0 \oplus x^* \oplus u^*$ pour (x^*, u^*) vérifiant les conditions (6.11).

Analysons la probabilité de succès de l'attaque. Quand $\mathcal{D}$ interagit avec le monde réel (EMSP_k^P, P), alors il répond toujours 1 puisque la paire (x^*, u^*) telle que $x^* \oplus u^* = k \oplus t_0$, où k est la clé principale, vérifie nécessairement les conditions (6.11). Cela peut être facilement vérifié à partir de la propriété de « commutativité » suivante, vraie pour tout $x \in \{0,1\}^n$:

$$k \oplus t_2 \oplus P(t_1 \oplus t_2 \oplus \mathsf{EMSP}_k^P(x)) = \mathsf{EMSP}_k^P(t_0 \oplus t_1 \oplus P(k \oplus t_0 \oplus x)).$$

Quand le distingueur interagit avec le monde idéal (E, P), où E est une permutation uniformément aléatoire et indépendante de P, alors si on fixe $P' = t_0 \oplus t_1 \oplus P$ et $E' = t_1 \oplus t_2 \oplus E$, l'équation (6.11) se simplifie en l'équation (6.10) où E et P sont remplacés par E' et P', de telle façon que l'on peut utiliser exactement la même analyse que pour l'attaque de la section 6.4.1. Ainsi, $\mathcal{D}$ répond 1 avec probabilité $\mathcal{O}(\frac{1}{N})$. On vient donc de prouver le théorème suivant :

Théorème 6.10. *Considérons le schéma d'Even-Mansour généralisé à 2 tours et 1 permutation* $\mathsf{EMSP}[n, 2, \ell = n, \boldsymbol{\gamma}]$ *dont les clés de tours* k_i *sont dérivées de la clé principale* k *en xorant par des constantes, c'est-à-dire* $\gamma_i(k) = k \oplus t_i$ *pour* $i = 1, 2, 3$*, pour des constantes publiques* (t_0, t_1, t_2)*. Alors il existe une attaque permettant de distinguer ce schéma d'une permutation uniformément aléatoire avec, au plus,* $2^{2+\frac{n}{2}}$ *requêtes à la permutation externe et* $2^{2+\frac{n}{2}}$ *requêtes à la permutation interne, et dont l'avantage est* $1 - \mathcal{O}(\frac{1}{N})$*.* ♢

6.5 Preuve de sécurité pour des permutations indépendantes et des clés de tours identiques

Dans cette section, on prouve une borne de sécurité en $\widetilde{\mathcal{O}}(2^{\frac{2n}{3}})$ pour le schéma d'Even-Mansour généralisé à 2 tours avec des permutations indépendantes et des clés de tours

identiques $\mathsf{EMIP}[n,2]$ (présenté en figure 6.3). Plus précisément, on prouve le théorème suivant :

Théorème 6.11 (Permutations indépendantes et clés de tours identiques). *On considère le schéma d'Even-Mansour généralisé à 2 tours avec des permutations indépendantes et des clés de tours identiques* $\mathsf{EMIP}[n,2]$. *Supposons que* $9n \leq q_e, q_p \leq N/2$ *et* $2q_e + 2q_p \leq N$. *Alors*

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{EMIP}[n,2]}(q_e, q_p) \leq \frac{6}{N} + \frac{2q_e^2 q_p + 7q_e q_p^2 + 4q_p^2\sqrt{q_e q_p}}{N^2} + \frac{9q_p\sqrt{nq_e}}{N}\,. \qquad \diamondsuit$$

Démonstration. Ce théorème est une conséquence directe des lemmes 6.1, 6.12 et 6.13 que nous prouvons ci-dessous. ∎

En posant $q = \max(q_e, q_p)$, la majoration du théorème 6.11 se simplifie en

$$\frac{6}{N} + \frac{13q^3}{N^2} + \frac{9\sqrt{n}q^{\frac{3}{2}}}{N} = \frac{6}{2^n} + \frac{13q^3}{2^{2n}} + \frac{9q^{\frac{3}{2}}}{2^{n-\frac{1}{2}\log_2 n}}\,.$$

Ainsi, le schéma est sûr jusqu'à $\mathcal{O}(2^{\frac{2n}{3}-\frac{1}{3}\log_2 n}) = \widetilde{\mathcal{O}}(2^{\frac{2n}{3}})$ requêtes.

Le reste de cette section est consacré à la preuve du théorème 6.11. En suivant la méthodologie présentée en section 6.2.4, la première étape consiste à définir un ensemble $\mathcal{T}_2$ de « mauvaises » transcriptions $\tau = (\mathcal{Q}_E, \mathcal{Q}_{P_1}, \mathcal{Q}_{P_2}, k)$, avec $|\mathcal{Q}_E| = q_e$ et $|\mathcal{Q}_{P_1}| = |\mathcal{Q}_{P_2}| = q_p$. De manière informelle, une transcription est mauvaise si la clé crée des chaînes de collisions de longueur 2, ce qui peut empêcher de connecter l'entrée à la sortie.

Définition 6.1 (Mauvaise transcription, cas des permutations indépendantes) On dit qu'une transcription $\tau = (\mathcal{Q}_E, \mathcal{Q}_{P_1}, \mathcal{Q}_{P_2}, k) \in \mathcal{T}$ est *mauvaise* si

$$k \in \mathsf{BadK} = \bigcup_{1\leq i\leq 3} \mathsf{BadK}_i$$

où :

$$k \in \mathsf{BadK}_1 \Leftrightarrow k = x \oplus u_1 = v_2 \oplus y \text{ pour } (x,y) \in \mathcal{Q}_E, (u_1,v_1) \in \mathcal{Q}_{P_1}, (u_2,v_2) \in \mathcal{Q}_{P_2}$$
$$k \in \mathsf{BadK}_2 \Leftrightarrow k = x \oplus u_1 = v_1 \oplus u_2 \text{ pour } (x,y) \in \mathcal{Q}_E, (u_1,v_1) \in \mathcal{Q}_{P_1}, (u_2,v_2) \in \mathcal{Q}_{P_2}$$
$$k \in \mathsf{BadK}_3 \Leftrightarrow k = v_1 \oplus u_2 = v_2 \oplus y \text{ pour } (x,y) \in \mathcal{Q}_E, (u_1,v_1) \in \mathcal{Q}_{P_1}, (u_2,v_2) \in \mathcal{Q}_{P_2}\,.$$

Sinon, τ est dite *bonne*. On note $\mathcal{T}_2$ l'ensemble des mauvaises transcriptions et $\mathcal{T}_1 = \mathcal{T} \setminus \mathcal{T}_2$ l'ensemble des bonnes transcriptions. ⧫

Remarquons que $k \in \mathsf{BadK}_1$ correspond au cas où $x \oplus k$ collisionne sur une entrée de P_1 et $y \oplus k$ collisionne sur une sortie de P_2, de telle façon que x s'envoie sur y si, de manière très improbable, k vaut exactement $v_1 \oplus u_2$. Ce cas peut être vu comme une chaîne de longueur 2 qui connecte P_1 à P_2 en passant par la permutation externe. Le cas $k \in \mathsf{BadK}_2$ correspond au cas d'une chaîne de longueur 2 qui part d'une entrée x ($x \oplus k = u_1$ puis $v_1 \oplus k = u_2$) ce qui, là encore, permet de connecter x à y uniquement si k vaut, de manière très improbable, $v_2 \oplus y$. Le cas $k \in \mathsf{BadK}_3$ correspond au cas d'une chaîne de longueur 2 qui part d'une sortie y et vérifie les mêmes propriétés de manière symétrique.

Nous commençons par majorer la probabilité d'obtenir une mauvaise transcription dans le monde idéal.

Lemme 6.12. *Supposons que $9n \leq q_e, q_p \leq N/2$. Alors :*

$$\Pr[T_{\mathrm{id}} \in \mathcal{T}_2] \leq \frac{6}{N} + \frac{2q_e^2 q_p + 3q_e q_p^2 + 4q_p^2\sqrt{q_e q_p}}{N^2} + \frac{9q_p\sqrt{nq_e}}{N}\,. \qquad \triangledown$$

Démonstration. Remarquons que dans le monde idéal, les ensembles BadK_1, BadK_2 et BadK_3 ne dépendent que des permutations uniformément aléatoires E, P_1, et P_2, et pas de la clé k qui est tirée uniformément aléatoire à la fin de l'interaction du distingueur avec (E, P_1, P_2). Ainsi, pour tous $C_1, C_2, C_3 > 0$, on a

$$\Pr[T_{\mathrm{id}} \in \mathcal{T}_2] \leq \sum_{i=1,2,3} \Pr\left[E, P_1, P_2 \leftarrow_{\$} \mathcal{P}_n : |\mathsf{BadK}_i| \geq C_i\right] + \frac{C_1 + C_2 + C_3}{N}\,.$$

Etant donnée une transcription de permutations $(\mathcal{Q}_E, \mathcal{Q}_{P_1}, \mathcal{Q}_{P_2})$, soit :

$$\begin{aligned} X &= \{x \in \{0,1\}^n : (x,y) \in \mathcal{Q}_E\}, & Y &= \{y \in \{0,1\}^n : (x,y) \in \mathcal{Q}_E\},\\ U_1 &= \{u_1 \in \{0,1\}^n : (u_1,v_1) \in \mathcal{Q}_{P_1}\}, & V_1 &= \{v_1 \in \{0,1\}^n : (u_1,v_1) \in \mathcal{Q}_{P_1}\},\\ U_2 &= \{u_2 \in \{0,1\}^n : (u_2,v_2) \in \mathcal{Q}_{P_2}\}, & V_2 &= \{v_2 \in \{0,1\}^n : (u_2,v_2) \in \mathcal{Q}_{P_2}\} \end{aligned}$$

les domaines et images de $\mathcal{Q}_E$, $\mathcal{Q}_{P_1}$, et $\mathcal{Q}_{P_2}$ respectivement. Alors, on a

$$\begin{aligned} |\mathsf{BadK}_1| &\leq \mu(\mathcal{Q}_E, U_1, V_2) \stackrel{\mathrm{def}}{=} |\{((x,y),u_1,v_2) \in \mathcal{Q}_E \times U_1 \times V_2 : x \oplus u_1 = v_2 \oplus y\}|\\ |\mathsf{BadK}_2| &\leq \mu(\mathcal{Q}_{P_1}, X, U_2) \stackrel{\mathrm{def}}{=} |\{((u_1,v_1),x,u_2) \in \mathcal{Q}_{P_1} \times X \times U_2 : x \oplus u_1 = v_1 \oplus u_2\}|\\ |\mathsf{BadK}_3| &\leq \mu(\mathcal{Q}_{P_2}, V_1, Y) \stackrel{\mathrm{def}}{=} |\{((u_2,v_2),v_1,y) \in \mathcal{Q}_{P_2} \times V_1 \times Y : v_1 \oplus u_2 = v_2 \oplus y\}|\,. \end{aligned}$$

On peut alors utiliser le théorème 6.5 (avec Γ l'identité) pour majorer $|\mathsf{BadK}_i|$ pour $i = 1, 2, 3$, avec forte probabilité (remarquons que, afin d'appliquer le théorème pour majorer, disons, $|\mathsf{BadK}_1|$, on considère la combinaison du distingueur $\mathcal{D}$ et des permutations P_1 et P_2 comme un adversaire probabiliste $\mathcal{A}$ interagissant avec la permutation E, produisant ainsi la transcription $\mathcal{Q}_E$). On obtient alors que, pour

$$\begin{aligned} C_1 &= \frac{q_e q_p^2}{N} + \frac{2q_e^2 q_p}{N} + 3q_p\sqrt{nq_e}\\ C_2 = C_3 &= \frac{q_e q_p^2}{N} + \frac{2q_p^2\sqrt{q_e q_p}}{N} + 3q_p\sqrt{nq_e}\,, \end{aligned}$$

on a $\Pr[E, P_1, P_2 \leftarrow_{\$} \mathcal{P}_n : |\mathsf{BadK}_i| \geq C_i] \leq 2/N$ pour $i = 1, 2, 3$, ce qui permet de conclure.■

Dans la deuxième partie de la preuve, on montre que, pour toute bonne transcription τ, le rapport entre la probabilité d'obtenir τ dans le monde idéal et la probabilité d'obtenir τ dans le monde réel est proche de 1.

Lemme 6.13. *Supposons que $2q_e + 2q_p \leq N$. Alors, pour tout $\tau \in \mathcal{T}_1$, on a :*

$$\frac{\Pr[T_{\mathrm{re}} = \tau]}{\Pr[T_{\mathrm{id}} = \tau]} \geq 1 - \frac{4q_e q_p^2}{N^2}\,. \qquad \triangledown$$

DÉMONSTRATION. Fixons une bonne transcription $\tau = (\mathcal{Q}_E, \mathcal{Q}_{P_1}, \mathcal{Q}_{P_2}, k) \in \mathcal{T}_1$. On définit :

$$\mathsf{p}(\tau) \stackrel{\text{def}}{=} \Pr\left[P_1, P_2 \leftarrow_{\$} \mathcal{P}_n : \mathsf{EMIP}_k^{P_1,P_2} \vdash \mathcal{Q}_E \,\middle|\, (P_1 \vdash \mathcal{Q}_{P_1}) \wedge (P_2 \vdash \mathcal{Q}_{P_2})\right],$$

de telle manière que, par le lemme 6.2,

$$\frac{\Pr[T_{\text{re}} = \tau]}{\Pr[T_{\text{id}} = \tau]} = (N)_{q_e} \cdot \mathsf{p}(\tau)\,. \tag{6.12}$$

Ainsi, on doit maintenant minorer $\mathsf{p}(\tau)$. Tout d'abord, on modifie les permutations internes P_1, P_2 et la transcription pour se « débarrasser » de la clé k. Pour cela, on définit :

$$\begin{aligned}
P_1' &= P_1 \oplus k \\
P_2' &= P_2 \oplus k \\
\mathcal{Q}_E' &= \{(x \oplus k, y) : (x, y) \in \mathcal{Q}_E\} \\
\mathcal{Q}_{P_1}' &= \{(u_1, v_1 \oplus k) : (u_1, v_1) \in \mathcal{Q}_{P_1}\} \\
\mathcal{Q}_{P_2}' &= \{(u_2, v_2 \oplus k) : (u_2, v_2) \in \mathcal{Q}_{P_2}\}\,.
\end{aligned}$$

Alors, on a clairement :

$$\mathsf{p}(\tau) = \Pr\left[P_1', P_2' \leftarrow_{\$} \mathcal{P}_n : P_2' \circ P_1' \vdash \mathcal{Q}_E' \,\middle|\, (P_1' \vdash \mathcal{Q}_{P_1}') \wedge (P_2' \vdash \mathcal{Q}_{P_2}')\right].$$

Soient :

$$\begin{aligned}
X &= \{x' \in \{0,1\}^n : (x', y') \in \mathcal{Q}_E'\}, & Y &= \{y' \in \{0,1\}^n : (x', y') \in \mathcal{Q}_E'\}, \\
U_1 &= \{u_1' \in \{0,1\}^n : (u_1', v_1') \in \mathcal{Q}_{P_1}'\}, & V_1 &= \{v_1' \in \{0,1\}^n : (u_1', v_1') \in \mathcal{Q}_{P_1}'\}, \\
U_2 &= \{u_2' \in \{0,1\}^n : (u_2', v_2') \in \mathcal{Q}_{P_2}'\}, & V_2 &= \{v_2' \in \{0,1\}^n : (u_2', v_2') \in \mathcal{Q}_{P_2}'\}
\end{aligned}$$

les domaines et les images de $\mathcal{Q}_E'$, $\mathcal{Q}_{P_1}'$, et $\mathcal{Q}_{P_2}'$ respectivement. On définit également $\alpha_1 = |V_2 \cap Y|$ et $\alpha_2 = |X \cap U_1|$. On peut maintenant réécrire que τ est une bonne transcription de la manière suivante (voir figure 6.4) :

$k \notin \mathsf{BadK}_1 \Leftrightarrow \mathcal{Q}_E'(X \cap U_1)$ est disjoint de $V_2 \Leftrightarrow (\mathcal{Q}_E')^{-1}(V_2 \cap Y)$ est disjoint de U_1
$k \notin \mathsf{BadK}_2 \Leftrightarrow \mathcal{Q}_{P_1}'(X \cap U_1)$ est disjoint de U_2
$k \notin \mathsf{BadK}_3 \Leftrightarrow (\mathcal{Q}_{P_2}')^{-1}(V_2 \cap Y)$ est disjoint de V_1.

Pour voir pourquoi la première équivalence est vraie, remarquons que :

$$\begin{aligned}
&\mathcal{Q}_E'(X \cap U_1) \cap V_2 \neq \emptyset \\
&\Leftrightarrow x' = u_1' \text{ et } y' = v_2' \text{ pour certains } (x', y') \in \mathcal{Q}_E', (u_1', v_1') \in \mathcal{Q}_{P_1}', \text{ et } (u_2', v_2') \in \mathcal{Q}_{P_2}' \\
&\Leftrightarrow k = x \oplus u_1 \text{ et } k = v_2 \oplus y \text{ pour certains } (x, y) \in \mathcal{Q}_E, (u_1, v_1) \in \mathcal{Q}_{P_1}, \text{ et } (u_2, v_2) \in \mathcal{Q}_{P_2} \\
&\Leftrightarrow k \in \mathsf{BadK}_1\,.
\end{aligned}$$

Les autres cas sont prouvés de manière similaire.

Cela nous permet de minorer $\mathsf{p}(\tau)$. En effet, soit E_1 l'événement « $P_1'(x') = u_2'$ pour chacune des α_1 paires de requêtes $((x', y'), (u_2', v_2')) \in \mathcal{Q}_E' \times \mathcal{Q}_{P_2}'$ telles que $y' = v_2'$ » (flèche rouge sur la figure 6.4). De la même manière, soit E_2 l'événement « $P_2'(v_1') = y'$

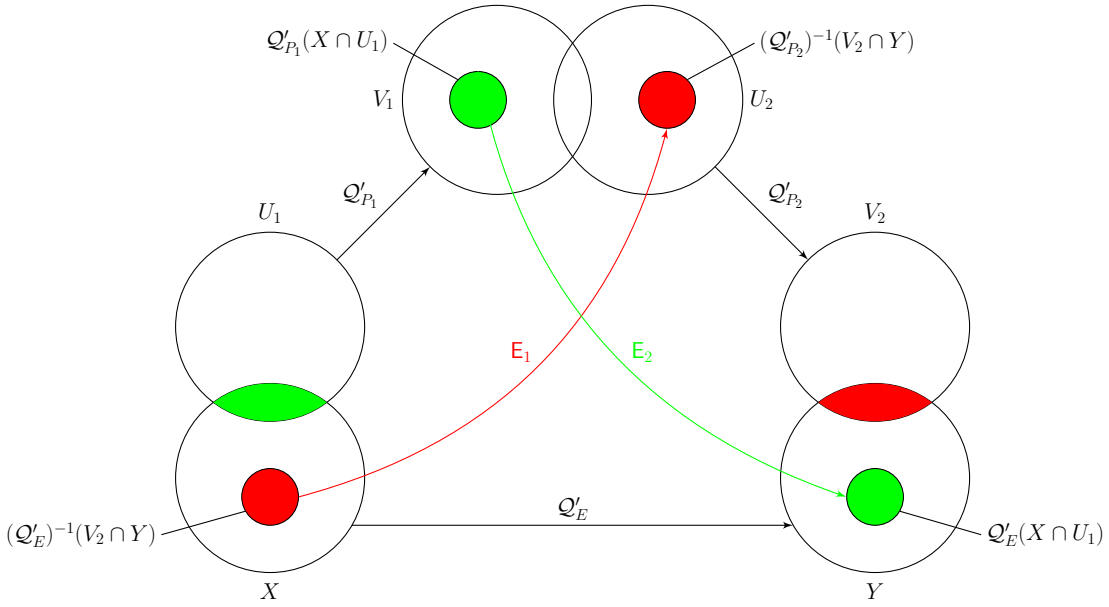

FIGURE 6.4 – Aide graphique pour la preuve du lemme 6.13. X et Y sont de taille q_e, tandis que U_1, V_1, U_2, et V_2 sont de taille q_p. Les zones rouges sont de taille α_1 et les zones vertes de taille α_2.

pour chacune des α_2 paires de requêtes $((x', y'), (u'_1, v'_1)) \in \mathcal{Q}'_E \times \mathcal{Q}'_{P_1}$ telles que $x' = u'_1$ » (flèche verte sur la figure 6.4). Puisque $P'_2 \circ P'_1 \vdash \mathcal{Q}'_E$ implique E_1 et E_2, on a

$$\begin{aligned}\mathsf{p}(\tau) &= \Pr\left[P'_1, P'_2 \leftarrow_\$ \mathcal{P}_n : (P'_2 \circ P'_1 \vdash \mathcal{Q}'_E) \wedge \mathsf{E}_1 \wedge \mathsf{E}_2 \middle| (P'_1 \vdash \mathcal{Q}'_{P_1}) \wedge (P'_2 \vdash \mathcal{Q}'_{P_2})\right] \\ &= \Pr\left[P'_1, P'_2 \leftarrow_\$ \mathcal{P}_n : P'_2 \circ P'_1 \vdash \mathcal{Q}'_E \middle| (P'_1 \vdash \mathcal{Q}'_{P_1}) \wedge (P'_2 \vdash \mathcal{Q}'_{P_2}) \wedge \mathsf{E}_1 \wedge \mathsf{E}_2\right] \\ &\quad \times \Pr\left[P'_1, P'_2 \leftarrow_\$ \mathcal{P}_n : \mathsf{E}_1 \wedge \mathsf{E}_2 \middle| (P'_1 \vdash \mathcal{Q}'_{P_1}) \wedge (P'_2 \vdash \mathcal{Q}'_{P_2})\right] . \qquad (6.13)\end{aligned}$$

De plus, puisque $(\mathcal{Q}'_E)^{-1}(V_2 \cap Y)$ est disjoint de U_1 et $(\mathcal{Q}'_{P_2})^{-1}(V_2 \cap Y)$ est disjoint de V_1, on a

$$\Pr\left[P'_1 \leftarrow_\$ \mathcal{P}_n : \mathsf{E}_1 \middle| P'_1 \vdash \mathcal{Q}'_{P_1}\right] = \frac{1}{(N - q_p)_{\alpha_1}} .$$

De la même manière, puisque $\mathcal{Q}'_{P_1}(X \cap U_1)$ est disjoint de U_2 et $\mathcal{Q}'_E(X \cap U_1)$ est disjoint de V_2, on a

$$\Pr\left[P'_2 \leftarrow_\$ \mathcal{P}_n : \mathsf{E}_2 \middle| P'_2 \vdash \mathcal{Q}'_{P_2}\right] = \frac{1}{(N - q_p)_{\alpha_2}} .$$

Ainsi,

$$\Pr\left[P'_1, P'_2 \leftarrow_\$ \mathcal{P}_n : \mathsf{E}_1 \wedge \mathsf{E}_2 \middle| (P'_1 \vdash \mathcal{Q}'_{P_1}) \wedge (P'_2 \vdash \mathcal{Q}'_{P_2})\right] = \frac{1}{(N - q_p)_{\alpha_1} \cdot (N - q_p)_{\alpha_2}} . \qquad (6.14)$$

Soit $\alpha = \alpha_1 + \alpha_2$. Conditionné sur l'événement $(P'_1 \vdash \mathcal{Q}'_{P_1}) \wedge (P'_2 \vdash \mathcal{Q}'_{P_2}) \wedge \mathsf{E}_1 \wedge \mathsf{E}_2$, P'_1 est fixé en $q_p + \alpha_1$ points, P'_2 est fixé en $q_p + \alpha_2$ points, et $P'_2 \circ P'_1$ coincide avec $\mathcal{Q}'_E$ pour α paires (x', y'). Il reste à minorer la probabilité p^* que $P'_2 \circ P'_1$ complète les $q_e - \alpha$ évaluations restantes et nécessaires pour étendre $\mathcal{Q}'_E$, c'est-à-dire

$$\mathsf{p}^* = \Pr\left[P'_1, P'_2 \leftarrow_\$ \mathcal{P}_n : P'_2 \circ P'_1 \vdash \mathcal{Q}'_E \middle| (P'_1 \vdash \mathcal{Q}'_{P_1}) \wedge (P'_2 \vdash \mathcal{Q}'_{P_2}) \wedge \mathsf{E}_1 \wedge \mathsf{E}_2\right] .$$

Soit S_1, respectivement T_1, l'ensemble des points pour lesquels P'_1, respectivement $(P'_1)^{-1}$, n'a pas été déterminée :

$$\begin{aligned} S_1 &= \{0,1\}^n \setminus (U_1 \sqcup (\mathcal{Q}'_E)^{-1}(V_2 \cap Y)) \\ T_1 &= \{0,1\}^n \setminus (V_1 \sqcup (\mathcal{Q}'_{P_2})^{-1}(V_2 \cap Y)) \,. \end{aligned}$$

De manière similaire, soit S_2, respectivement T_2, l'ensemble des points pour lesquels P'_2, respectivement $(P'_2)^{-1}$, n'a pas été déterminée :

$$\begin{aligned} S_2 &= \{0,1\}^n \setminus (U_2 \sqcup \mathcal{Q}'_{P_1}(X \cap U_1)) \\ T_2 &= \{0,1\}^n \setminus (V_2 \sqcup \mathcal{Q}'_E(X \cap U_1) \,. \end{aligned}$$

Et on pose

$$\begin{aligned} X' &= X \cap S_1 = X \setminus (U_1 \sqcup (\mathcal{Q}'_E)^{-1}(V_2 \cap Y)) \\ Y' &= Y \cap T_2 = Y \setminus (V_2 \sqcup \mathcal{Q}'_E(X \cap U_1)) \,. \end{aligned}$$

Alors p^* est exactement la probabilité que, sur le choix de deux bijections aléatoires $\overline{P'_1}$: $S_1 \to T_1$ et $\overline{P'_2} : S_2 \to T_2$, $\overline{P'_2} \circ \overline{P'_1}(x') = y'$ pour tout $(x', y') \in \mathcal{Q}'_E$ tel que $x' \in X'$ et $y' \in Y'$. On minore maintenant p^*.

Remarquons que $|X'| = |Y'| = q_e - \alpha$. Choisissons un ensemble $W \subseteq \{0,1\}^n \setminus (V_1 \cup U_2)$ de taille $q_e - \alpha$ (remarquons que $N - 2q_p \geq q_e - \alpha$ puisque, par hypothèse, $2q_e + 2q_p \leq N$) et une bijection $F : X' \to W$. Le nombre de paires possibles (W, F) est au moins

$$\binom{N - 2q_p}{q_e - \alpha} (q_e - \alpha)! = (N - 2q_p)_{q_e - \alpha} \,.$$

Pour chaque choix de (W, F), la probabilité que des bijections aléatoires $\overline{P'_1} : S_1 \to T_1$ et $\overline{P'_2} : S_2 \to T_2$ vérifient :

(1) $\overline{P'_1}(x') = F(x')$ pour chaque $x' \in X'$,

(2) $\overline{P'_2} \circ \overline{P'_1}(x') = y'$ pour chaque $(x', y') \in \mathcal{Q}'_E$ tel que $x' \in X'$ et $y' \in Y'$

est exactement

$$\frac{1}{(N - q_p - \alpha_1)_{q_e - \alpha} (N - q_p - \alpha_2)_{q_e - \alpha}} \,,$$

puisque la condition (1) fixe $q_e - \alpha$ équations distinctes sur $\overline{P'_1}$ et la condition (2) fixe $q_e - \alpha$ équations distinctes sur $\overline{P'_2}$. Ainsi, en sommant sur toutes les paires possibles (W, F), on obtient

$$\mathsf{p}^* \geq \frac{(N - 2q_p)_{q_e - \alpha}}{(N - q_p - \alpha_1)_{q_e - \alpha} (N - q_p - \alpha_2)_{q_e - \alpha}} \,. \tag{6.15}$$

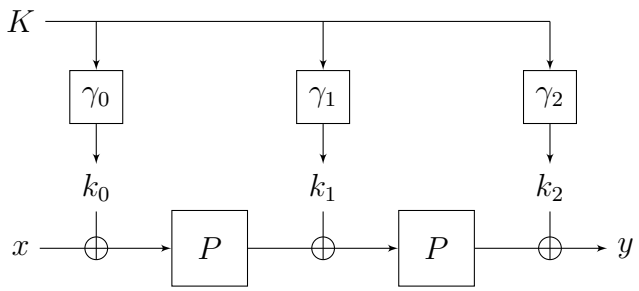

FIGURE 6.5 – Le schéma d'Even-Mansour généralisé pour deux tours et une permutation.

En combinant (6.12), (6.13), (6.14), et (6.15), on déduit que

$$\begin{aligned}
\frac{\Pr[T_{\mathrm{re}} = \tau]}{\Pr[T_{\mathrm{id}} = \tau]} &\geq \frac{(N)_{q_e}(N-2q_p)_{q_e-\alpha}}{(N-q_p)_{\alpha_1}(N-q_p-\alpha_1)_{q_e-\alpha}(N-q_p)_{\alpha_2}(N-q_p-\alpha_2)_{q_e-\alpha}} \\
&= \frac{(N)_{q_e}(N-2q_p)_{q_e-\alpha}}{(N-q_p)_{q_e-\alpha_2}(N-q_p)_{q_e-\alpha_1}} \\
&= \frac{(N)_{q_e}(N-2q_p)_{q_e}}{(N-q_p)_{q_e}(N-q_p)_{q_e}} \times \underbrace{\frac{(N-q_p-q_e+\alpha_2)_{\alpha_2}(N-q_p-q_e+\alpha_1)_{\alpha_1}}{(N-2q_p-q_e+\alpha)_{\alpha}}}_{\geq 1} \\
&\geq \frac{(N)_{q_e}(N-2q_p)_{q_e}}{((N-q_p)_{q_e})^2} \\
&\geq 1 - \frac{4q_e q_p^2}{N^2}\,,
\end{aligned}$$

où la dernière inégalité provient du lemme 6.3 avec $a = q_e$ et $b = c = d = q_p$, et l'hypothèse que $2q_e + 2q_p \leq N$. Ce qui permet de conclure. ∎

6.6 Preuve de sécurité pour le cas d'une seule permutation

Dans cette section, on étudie la sécurité du schéma d'Even-Mansour généralisé $\mathsf{EMSP}[n, r, \ell, \boldsymbol{\gamma}]$ où une seule permutation P est utilisée au lieu de deux permutations indépendantes (voir figure 6.5). Les résultats de la section 6.4 impliquent qu'on ne peut pas utiliser la même clé k à chaque tour si l'on vise une sécurité au delà de la borne des anniversaires. Ainsi, une dérivation de clés non-triviale $\boldsymbol{\gamma} = (\gamma_0, \gamma_1, \gamma_2)$, avec $\gamma_i : \{0,1\}^\ell \to \{0,1\}^n$, est nécessaire (on reste, dans un premier temps, le plus général possible avant de spécifier $(\gamma_0, \gamma_1, \gamma_2)$). Etant donné une clé $K \in \{0,1\}^\ell$, on note $k_0 = \gamma_0(K)$, $k_1 = \gamma_1(K)$, et $k_2 = \gamma_2(K)$, tels que :

$$\mathsf{EMSP}_K^P(x) = P(P(x \oplus k_0) \oplus k_1) \oplus k_2\,.$$

6.6.1 Bonnes transcriptions et leurs propriétés

Soit $\tau = (\mathcal{Q}_E, \mathcal{Q}_P, K)$, avec $|\mathcal{Q}_E| = q_e$, $|\mathcal{Q}_P| = q_p$, et $K \in \{0,1\}^\ell$, une transcription atteignable. Comme précédemment, on commence par définir les mauvaises transcriptions. Dans tout ce qui suit, on pose

$$M = \frac{q_e}{N^{\frac{1}{3}}}\,.$$

Définition 6.2 (Mauvaise transcription, cas d'une seule permutation)
On dit qu'une transcription $\tau = (\mathcal{Q}_E, \mathcal{Q}_P, K) \in \mathcal{T}$ est *mauvaise* si

$$K \in \mathsf{BadK} = \bigcup_{1 \le i \le 10} \mathsf{BadK}_i$$

où

$$\begin{aligned}
K \in \mathsf{BadK}_1 &\Leftrightarrow k_0 = x \oplus u \text{ et } k_2 = v' \oplus y \text{ pour certains } (x,y) \in \mathcal{Q}_E \text{ et } (u,v),(u',v') \in \mathcal{Q}_P \\
K \in \mathsf{BadK}_2 &\Leftrightarrow k_0 = x \oplus u \text{ et } k_1 = v \oplus u' \text{ pour certains } (x,y) \in \mathcal{Q}_E \text{ et } (u,v),(u',v') \in \mathcal{Q}_P \\
K \in \mathsf{BadK}_3 &\Leftrightarrow k_1 = v \oplus u' \text{ et } k_2 = v' \oplus y \text{ pour certains } (x,y) \in \mathcal{Q}_E \text{ et } (u,v),(u',v') \in \mathcal{Q}_P \\
K \in \mathsf{BadK}_4 &\Leftrightarrow k_0 = x \oplus u \text{ et } k_0 \oplus k_1 = v \oplus x' \text{ pour certains } (x,y),(x',y') \in \mathcal{Q}_E, (u,v) \in \mathcal{Q}_P \\
K \in \mathsf{BadK}_5 &\Leftrightarrow k_1 \oplus k_2 = y' \oplus u \text{ et } k_2 = v \oplus y \text{ pour certains } (x,y),(x',y') \in \mathcal{Q}_E, (u,v) \in \mathcal{Q}_P \\
K \in \mathsf{BadK}_6 &\Leftrightarrow |\{((x,y),(u,v)) \in \mathcal{Q}_E \times \mathcal{Q}_P : x \oplus u = k_0\}| > \frac{M}{3} \\
K \in \mathsf{BadK}_7 &\Leftrightarrow |\{((x,y),(u,v)) \in \mathcal{Q}_E \times \mathcal{Q}_P : v \oplus y = k_2\}| > \frac{M}{3} \\
K \in \mathsf{BadK}_8 &\Leftrightarrow |\{((x,y),(u,v)) \in \mathcal{Q}_E \times \mathcal{Q}_P : x \oplus v = k_0 \oplus k_1\}| > \frac{M}{3} \\
K \in \mathsf{BadK}_9 &\Leftrightarrow |\{((x,y),(u,v)) \in \mathcal{Q}_E \times \mathcal{Q}_P : u \oplus y = k_1 \oplus k_2\}| > \frac{M}{3} \\
K \in \mathsf{BadK}_{10} &\Leftrightarrow \left|\{((x,y),(x',y')) \in \mathcal{Q}_E \times \mathcal{Q}_E : x \oplus y' = k_0 \oplus k_1 \oplus k_2\}\right| > M\,.
\end{aligned}$$

Sinon τ est dite *bonne*. On note $\mathcal{T}_2$ l'ensemble des mauvaises transcriptions et $\mathcal{T}_1 = \mathcal{T} \setminus \mathcal{T}_2$ l'ensemble des bonnes transcriptions. ♦

On reporte l'étude de la probabilité d'obtenir une mauvaise transcription à la prochaine section et nous nous concentrons sur les propriétés d'une bonne transcription. Nous allons prouver le lemme suivant :

Lemme 6.14. *Supposons que $N \ge 7^3$ et $4q_e + 2q_p \le N$. Soit $\tau = (\mathcal{Q}_E, \mathcal{Q}_P, K) \in \mathcal{T}_1$ une bonne transcription. Alors*

$$\frac{\Pr[T_{\mathrm{re}} = \tau]}{\Pr[T_{\mathrm{id}} = \tau]} \ge 1 - \varepsilon_1\,,$$

où

$$\varepsilon_1 = \frac{4q_e(q_e+q_p)^2}{N^2} + \frac{2q_e^2}{N^{\frac{4}{3}}} + \frac{20q_e}{N^{\frac{2}{3}}}\,.$$ ▽

Démonstration. Fixons une bonne transcription $\tau = (\mathcal{Q}_E, \mathcal{Q}_P, K) \in \mathcal{T}_1$. On pose

$$\mathsf{p}(\tau) \stackrel{\text{def}}{=} \Pr\left[P \leftarrow_{\$} \mathcal{P}_n : \mathsf{EMSP}_K^P \vdash \mathcal{Q}_E \middle| P \vdash \mathcal{Q}_P\right]\,,$$

de telle façon que le lemme 6.2 permet d'écrire

$$\frac{\Pr[T_{\mathrm{re}} = \tau]}{\Pr[T_{\mathrm{id}} = \tau]} = (N)_{q_e} \cdot \mathsf{p}(\tau)\,. \tag{6.16}$$

Notre objectif est de minorer $\mathsf{p}(\tau)$. On commence par modifier la permutation interne P et la transcription pour se débarrasser des clés de tours :

$$\begin{aligned} P' &= P \oplus k_1\,, \\ \mathcal{Q}'_E &= \{(x \oplus k_0, y \oplus k_1 \oplus k_2) : (x,y) \in \mathcal{Q}_E\}\,, \\ \mathcal{Q}'_P &= \{(u, v \oplus k_1) : (u,v) \in \mathcal{Q}_P\}\,. \end{aligned}$$

Ainsi :

$$\mathsf{p}(\tau) = \Pr\left[P' \leftarrow_{\$} \mathcal{P}_n : P' \circ P' \vdash \mathcal{Q}'_E | P' \vdash \mathcal{Q}'_P\right]\,.$$

Soient

$$\begin{aligned} X &= \{x' \in \{0,1\}^n : (x',y') \in \mathcal{Q}'_E\}, & Y &= \{y' \in \{0,1\}^n : (x',y') \in \mathcal{Q}'_E\}, \\ U &= \{u' \in \{0,1\}^n : (u',v') \in \mathcal{Q}'_P\}, & V &= \{v' \in \{0,1\}^n : (u',v') \in \mathcal{Q}'_P\} \end{aligned}$$

les domaines et les images de $\mathcal{Q}'_E$ et $\mathcal{Q}'_P$, respectivement. On note $\alpha_1 = |Y \cap V|$ et $\alpha_2 = |X \cap U|$. On peut réécrire le fait que la transcription est bonne de la façon suivante (voir figure 6.6) :

$$K \notin \mathsf{BadK}_1 \Leftrightarrow \mathcal{Q}'_E(X \cap U) \text{ est disjoint de } V \Leftrightarrow (\mathcal{Q}'_E)^{-1}(Y \cap V) \text{ est disjoint de } U \quad \text{(B.1)}$$

$$K \notin \mathsf{BadK}_2 \Leftrightarrow \mathcal{Q}'_P(X \cap U) \text{ est disjoint de } U \quad \text{(B.2)}$$

$$K \notin \mathsf{BadK}_3 \Leftrightarrow (\mathcal{Q}'_P)^{-1}(Y \cap V) \text{ est disjoint de } V \quad \text{(B.3)}$$

$$K \notin \mathsf{BadK}_4 \Leftrightarrow \mathcal{Q}'_P(X \cap U) \text{ est disjoint de } X \quad \text{(B.4)}$$

$$K \notin \mathsf{BadK}_5 \Leftrightarrow (\mathcal{Q}'_P)^{-1}(Y \cap V) \text{ est disjoint de } Y \quad \text{(B.5)}$$

$$K \notin \mathsf{BadK}_6 \Leftrightarrow \alpha_2 = |X \cap U| \leq \frac{M}{3} \quad \text{(B.6)}$$

$$K \notin \mathsf{BadK}_7 \Leftrightarrow \alpha_1 = |Y \cap V| \leq \frac{M}{3} \quad \text{(B.7)}$$

$$K \notin \mathsf{BadK}_8 \Leftrightarrow |X \cap V| \leq \frac{M}{3} \quad \text{(B.8)}$$

$$K \notin \mathsf{BadK}_9 \Leftrightarrow |Y \cap U| \leq \frac{M}{3} \quad \text{(B.9)}$$

$$K \notin \mathsf{BadK}_{10} \Leftrightarrow |X \cap Y| \leq M\,. \quad \text{(B.10)}$$

Soit E_1 l'événement « $P'(x') = u'$ pour chacune des α_1 paires de requêtes $((x',y'),(u',v')) \in \mathcal{Q}'_E \times \mathcal{Q}'_P$ telles que $y' = v'$ » (les flèches rouges sur la figure 6.6). De manière similaire, soit E_2 l'événement « $P'(v') = y'$ pour chacune des α_2 paires de requêtes $((x',y'),(u',v')) \in \mathcal{Q}'_E \times \mathcal{Q}'_P$ telles que $x' = u'$ (les flèches vertes sur la figure 6.6). Puisque $P' \circ P' \vdash \mathcal{Q}'_E$ implique E_1 et E_2, on a

$$\begin{aligned} \mathsf{p}(\tau) &= \Pr\left[P' \leftarrow_{\$} \mathcal{P}_n : (P' \circ P' \vdash \mathcal{Q}'_E) \wedge \mathsf{E}_1 \wedge \mathsf{E}_2 | P' \vdash \mathcal{Q}'_P\right] \\ &= \Pr\left[P' \leftarrow_{\$} \mathcal{P}_n : P' \circ P' \vdash \mathcal{Q}'_E | (P' \vdash \mathcal{Q}'_P) \wedge \mathsf{E}_1 \wedge \mathsf{E}_2\right] \\ &\quad \times \Pr\left[P' \leftarrow_{\$} \mathcal{P}_n : \mathsf{E}_1 \wedge \mathsf{E}_2 | P' \vdash \mathcal{Q}'_P\right]\,. \end{aligned} \quad \text{(6.17)}$$

Remarquons que :

1. U, $\mathcal{Q}'_P(X \cap U)$, et $(\mathcal{Q}'_E)^{-1}(Y \cap V)$ sont deux à deux disjoints puisque :
   – U et $(\mathcal{Q}'_E)^{-1}(Y \cap V)$ sont disjoints par (B.1),

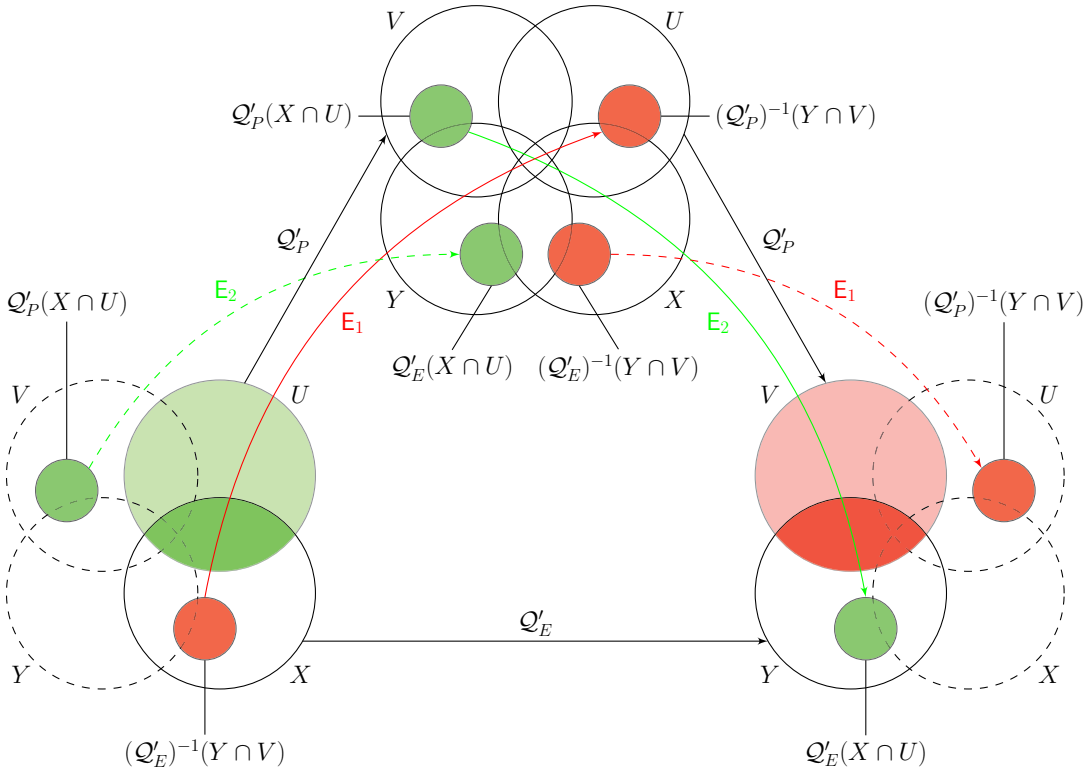

FIGURE 6.6 – Aide graphique pour la preuve du lemme 6.14. X et Y sont de taille q_e, tandis que U et V sont de taille q_p. Les zones rouges sont de taille α_1 et les zones vertes sont de taille α_2. Conditionné sur $(P' \vdash \mathcal{Q}'_P) \wedge \mathsf{E}_1 \wedge \mathsf{E}_2$, P' est défini sur les zones colorées de la partie gauche, tandis que $(P')^{-1}$ est défini sur les zones colorées de la partie droite.

– U et $\mathcal{Q}'_P(X \cap U)$ sont disjoints par (B.2),
– $(\mathcal{Q}'_E)^{-1}(Y \cap V)$ est contenu dans X, et X et $\mathcal{Q}'_P(X \cap U)$ sont disjoints par (B.4) ;

2. V, $\mathcal{Q}'_E(X \cap U)$, et $(\mathcal{Q}'_P)^{-1}(Y \cap V)$ sont deux à deux disjoints puisque :
– V et $\mathcal{Q}'_E(X \cap U)$ sont disjoints par (B.1),
– V et $(\mathcal{Q}'_P)^{-1}(Y \cap V)$ sont disjoints par (B.3),
– $\mathcal{Q}'_E(X \cap U)$ est contenu dans Y, et Y et $(\mathcal{Q}'_P)^{-1}(Y \cap V)$ sont disjoints par (B.5).

Ainsi, on a

$$\Pr\left[P' \leftarrow_\$ \mathcal{P}_n : \mathsf{E}_1 \wedge \mathsf{E}_2 | P' \vdash \mathcal{Q}'_P\right] = \frac{1}{(N - q_p)_{\alpha_1+\alpha_2}} . \tag{6.18}$$

Soit $\alpha = \alpha_1 + \alpha_2$. Conditionné sur l'événement $(P' \vdash \mathcal{Q}'_P) \wedge \mathsf{E}_1 \wedge \mathsf{E}_2$, P' est fixé en $q_p + \alpha$ points, et $P' \circ P'$ coincide avec $\mathcal{Q}'_E$ en α paires (x', y'). Il reste à minorer la probabilité p^* que $P' \circ P'$ complète $q_e - \alpha$ évaluations restantes et nécessaires pour étendre $\mathcal{Q}'_E$, à savoir

$$\mathsf{p}^* = \Pr\left[P' \leftarrow_\$ \mathcal{P}_n : P' \circ P' \vdash \mathcal{Q}'_E | (P' \vdash \mathcal{Q}'_P) \wedge \mathsf{E}_1 \wedge \mathsf{E}_2\right] .$$

Soit $S \subseteq \{0,1\}^n$ l'ensemble des points pour lesquels P' n'a pas été déterminée :

$$S = \{0,1\}^n \setminus (U \sqcup \mathcal{Q}'_P(X \cap U) \sqcup (\mathcal{Q}'_E)^{-1}(Y \cap V)) ,$$

et $T \subseteq \{0,1\}^n$ l'ensemble des points pour lesquels $(P')^{-1}$ n'a pas été déterminée :

$$T = \{0,1\}^n \setminus (V \sqcup \mathcal{Q}'_E(X \cap U) \sqcup (\mathcal{Q}'_P)^{-1}(Y \cap V)) .$$

Soient

$$\begin{aligned} X' &= X \cap S = X \setminus (U \sqcup (\mathcal{Q}'_E)^{-1}(Y \cap V)) \\ Y' &= Y \cap T = Y \setminus (V \sqcup \mathcal{Q}'_E(X \cap U)) . \end{aligned}$$

(Remarquons que $\mathcal{Q}'_E(X') = Y'$.) Alors p^* est exactement la probabilité que $\overline{P'} \circ \overline{P'}(x') = y'$ pour chaque $(x', y') \in \mathcal{Q}'_E$ tel que $x' \in X'$ et $y' \in Y'$, sur les choix aléatoires de la bijection $\overline{P'} : S \to T$. Remarquons que

1. $|S| = |T| = N - q_p - \alpha$;
2. $|X'| = |Y'| = q_e - \alpha$;
3. $|X' \cap Y'| \leq |X \cap Y| \leq M$ par (B.10) ;
4. $|X' \setminus T| \leq M$ puisque

$$\begin{aligned} X' \setminus T \subseteq X \setminus T &= X \cap \overline{T} \\ &= (X \cap V) \sqcup (X \cap \mathcal{Q}'_E(X \cap U)) \sqcup (X \cap (\mathcal{Q}'_P)^{-1}(Y \cap V)) \\ &\subseteq (X \cap V) \sqcup \mathcal{Q}'_E(X \cap U) \sqcup (\mathcal{Q}'_P)^{-1}(Y \cap V) , \end{aligned}$$

et $|X \cap V|$, $|X \cap U|$, et $|Y \cap V|$ sont au plus égal à $M/3$ par (B.8), (B.6), et (B.7), respectivement ;

5. $|Y' \setminus S| \leq M$ puisque

$$\begin{aligned} Y' \setminus S \subseteq Y \setminus S &= Y \cap \overline{S} \\ &= (Y \cap U) \sqcup (Y \cap \mathcal{Q}'_P(X \cap U)) \sqcup (Y \cap (\mathcal{Q}'_E)^{-1}(Y \cap V)) \\ &\subseteq (Y \cap U) \sqcup \mathcal{Q}'_P(X \cap U) \sqcup (\mathcal{Q}'_E)^{-1}(Y \cap V) , \end{aligned}$$

et $|Y \cap U|$, $|X \cap U|$, et $|Y \cap V|$ sont au plus égal à $M/3$ par (B.9), (B.6), et (B.7), respectivement.

Récapitulons le problème de minorer p^*. On note $q = q_e - \alpha$ et $q' = q_p + \alpha$. Soient N, q, q' des entiers positifs et $M > 0$. Soient S, $T \subseteq \{0,1\}^n$, où $|S| = |T| = N - q'$. Soit également $X' = \{x_1, \ldots, x_q\} \subseteq S$ et $Y' = \{y_1, \ldots, y_q\} \subseteq T$ des ensembles de taille q. Supposons que

$$|X' \cap Y'|, |X' \setminus T|, \text{ et } |Y' \setminus S| \leq M\,, \tag{A.1}$$
$$6M \leq q\,, \tag{A.2}$$
$$4q + 2q' \leq N\,. \tag{A.3}$$

Le problème est de trouver un minorant de la probabilité p^* qu'une bijection aléatoire P de S dans T vérifie $P(P(x_i)) = y_i$ pour tout $i = 1, \ldots, q$. ◇

Dans le lemme 6.15, nous allons prouver la minoration

$$\mathsf{p}^* \geq \frac{1}{(N)_q}\left(1 - \frac{14M^2}{q} - \frac{3q^2}{MN} - \frac{4q(q+q')^2}{N^2}\right). \tag{6.19}$$

Avant de prouver (6.19), on termine la preuve du lemme 6.16. Remarquons que les hypothèses (A.1), (A.2), et (A.3) nécessaires pour utiliser (6.19) sont vérifiées :

- l'hypothèse (A.1) est vérifiée car on suppose que τ est bonne ;
- $\alpha \leq M$ par (B.6) et (B.7) puisque τ est bonne, et par l'hypothèse de départ que $N \geq 7^3$, on a $7M \leq q_e$, de sorte que $6M \leq q_e - M \leq q_e - \alpha = q$, et l'hypothèse (A.2) est donc vérifiée ;
- par notre hypothèse de départ que $4q_e + 2q_p \leq N$, l'hypothèse (A.3) est vérifiée.

Ainsi, en combinant (6.16), (6.17), (6.18), et (6.19), on a

$$\frac{\Pr[T_{\text{re}} = \tau]}{\Pr[T_{\text{id}} = \tau]} \geq \frac{(N)_{q_e}}{(N)_{q_e-\alpha}(N-q_p)_\alpha}\left(1 - \frac{14M^2}{q_e - \alpha} - \frac{3(q_e-\alpha)^2}{MN} - \frac{4(q_e-\alpha)(q_e+q_p)^2}{N^2}\right).$$

Et, puisque

$$\frac{(N)_{q_e}}{(N)_{q_e-\alpha}(N-q_p)_\alpha} = \frac{(N-q_e+\alpha)_\alpha}{(N-q_p)_\alpha} \geq \frac{(N-q_e)_\alpha}{(N)_\alpha} \geq 1 - \frac{q_e\alpha}{N-\alpha+1} \geq 1 - \frac{Mq_e}{N-M}\,,$$

on obtient

$$\frac{\Pr[T_{\text{re}} = \tau]}{\Pr[T_{\text{id}} = \tau]} \geq 1 - \frac{Mq_e}{N-M} - \frac{14M^2}{q_e - M} - \frac{3q_e^2}{MN} - \frac{4q_e(q_e+q_p)^2}{N^2}\,.$$

En remplaçant M par $q_e/N^{\frac{1}{3}}$, et en notant que $N - M \geq N/2$ et $q_e - M \geq 6q_e/7$, on obtient finalement

$$\frac{\Pr[T_{\text{re}} = \tau]}{\Pr[T_{\text{id}} = \tau]} \geq 1 - \varepsilon_1$$

où

$$\varepsilon_1 = \frac{4q_e(q_e+q_p)^2}{N^2} + \frac{2q_e^2}{N^{\frac{4}{3}}} + \frac{20q_e}{N^{\frac{2}{3}}}\,.$$

Ce qui termine la preuve. ■

Il reste à prouver la réponse du problème défini précédemment, ce que nous faisons dans le lemme suivant :

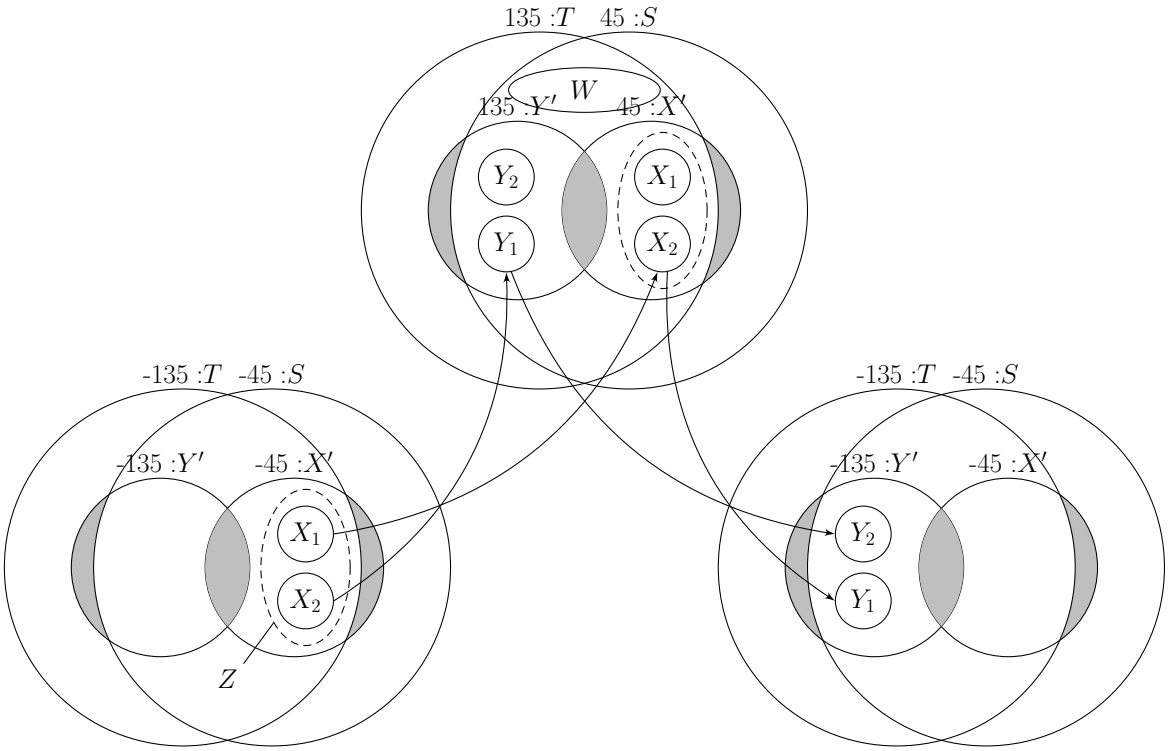

FIGURE 6.7 – Aide graphique pour la preuve du lemme 6.15. S et T sont de taille $N - q'$, tandis que X' et Y' sont de taille q. Les zones grises $X' \cap Y'$, $X' \setminus T$, et $Y' \setminus S$ sont de taille M. Les ensembles X_1, X_2, Y_1, Y_2 sont chacun de taille k. L'ensemble W est de taille $q - 2k$.

Lemme 6.15. *Soient N, q, q' des entiers positifs et $M > 0$. Soient S, $T \subseteq \{0,1\}^n$, où $|S| = |T| = N - q'$. Soit également $X' = \{x_1, \ldots, x_q\} \subseteq S$ et $Y' = \{y_1, \ldots, y_q\} \subseteq T$ des ensembles de taille q. Supposons que*

$$|X' \cap Y'|, |X' \setminus T|, \text{ et } |Y' \setminus S| \leq M\,, \tag{A.1}$$
$$6M \leq q\,, \tag{A.2}$$
$$4q + 2q' \leq N\,. \tag{A.3}$$

Soit p^* la probabilité qu'une bijection aléatoire P de S dans T vérifie $P(P(x_i)) = y_i$ pour tout $i = 1, \ldots, q$.[2] *Alors*

$$\mathsf{p}^* \geq \frac{1}{(N)_q}\left(1 - \frac{14M^2}{q} - \frac{3q^2}{MN} - \frac{4q(q+q')^2}{N^2}\right)\,. \qquad \triangledown$$

Démonstration. Le lecteur peut s'aider de la figure 6.7 pour mieux comprendre la preuve. Une façon simple de minorer p^* serait de ne compter que les bijections P telles que $P(X') \cap X' = \emptyset$. Néanmoins, cela n'est pas suffisant car cela donne une borne en q^2/N. Ainsi, on doit également compter les bijections P telles que $P(X') \cap X' \neq \emptyset$. ($P(X') \cap X'$ sera égal à X_2 dans la preuve suivante).

Soit $Z \subseteq X'$ défini comme

$$\begin{aligned} Z &= \{x_i \in X' : x_i \in T \wedge x_i \notin Y' \wedge y_i \in S \wedge y_i \notin X'\} \\ &= X' \setminus (\overline{T} \cup Y' \cup \{x_i \in X' : y_i \in Y' \setminus S\} \cup \{x_i \in X' : y_i \in X' \cap Y'\}) \\ &= X' \setminus ((X' \setminus T) \cup (X' \cap Y') \cup \{x_i \in X' : y_i \in Y' \setminus S\} \cup \{x_i \in X' : y_i \in X' \cap Y'\})\,. \end{aligned}$$

Soit $q'' = |Z|$. Puisque, par l'hypothèse (A.1), on a $|X' \cap Y'|$, $|X' \setminus T|$, et $|Y' \setminus S| \leq M$, on en déduit que $q'' \geq q - 4\lfloor M \rfloor \geq 2\lfloor M \rfloor$, où la dernière inégalité provient de l'hypothèse (A.2) qui implique que $6\lfloor M \rfloor \leq q$.

Pour chaque $0 \leq k \leq M$, on choisit deux sous-ensembles disjoints X_1, $X_2 \subset Z$ de taille k. On note

$$\begin{aligned} X_1 &= \{x_{i_1}, \ldots, x_{i_k}\} \\ X_2 &= \{x_{i_{k+1}}, \ldots, x_{i_{2k}}\} \\ X' \setminus (X_1 \cup X_2) &= \{x_{i_{2k+1}}, \ldots, x_{i_q}\} \end{aligned}$$

où $i_1 < \cdots < i_k$ et $i_{k+1} < \cdots < i_{2k}$ et $i_{2k+1} < \cdots < i_q$. Etant donné (X_1, X_2), on choisit une bijection $F : X_1 \to X_2$ telle que $F(X_1) = X_2$. Le nombre de possibilités pour (X_1, X_2, F) est

$$\binom{q''}{k}\binom{q''-k}{k}k! = \frac{(q'')_{2k}}{k!}\,. \tag{6.20}$$

Pour chaque paire d'ensembles (X_1, X_2), soit $Y_1 = \{y_{i_1}, \ldots, y_{i_k}\}$ et $Y_2 = \{y_{i_{k+1}}, \ldots, y_{i_{2k}}\}$. Pour une paire fixée d'ensembles (X_1, X_2), on choisit également

$$W \subset (S \cap T) \setminus (X' \cup Y')$$

2. Si $P(x_i) \notin S$, alors $P(P(x_i))$ est considérée comme indéfinie.

tel que $|W| = q - 2k$. C'est possible (c'est-à-dire $(S \cap T) \setminus (X' \cup Y')$ est assez grand) puisque, par l'hypothèse (A.3), $N \geq 3q + 2q'$, de sorte que, pour $0 \leq k \leq M$, on a

$$|(S \cap T) \setminus (X' \cup Y')| \geq |S \cap T| - |X' \cup Y'| \geq (N - 2q') - 2q \geq q - 2k\,.$$

Pour chaque choix de W, on choisit également une bijection $G : X' \setminus (X_1 \cup X_2) \to W$. Alors, le nombre de possibilités pour la paire (W, G) est au moins

$$\binom{N - 2q - 2q'}{q - 2k} \times (q - 2k)! = (N - 2q - 2q')_{q-2k}\,. \tag{6.21}$$

Pour chaque choix de (X_1, X_2, F, W, G), la probabilité qu'une bijection aléatoire $P : S \to T$ vérifie

(1) $P(x) = F(x)$ pour chaque $x \in X_1$,

(2) $P(x) = G(x)$ pour chaque $x \in X' \setminus (X_1 \cup X_2)$,

(3) $P(P(x_i)) = y_i$ pour tout $i = 1, \ldots, q$

est exactement

$$\frac{1}{(N - q')_{2q-k}}\,. \tag{6.22}$$

En effet, notons $\Pi : X' \to Y'$ la bijection telle que $\Pi(x_i) = y_i$ pour $i = 1, \ldots, q$. Alors une bijection $P : S \to T$ vérifie (1), (2) et (3) ci-dessus si et seulement si (voir également la figure 6.7) :

i) $P(x) = F(x)$ pour chaque $x \in X_1$, ce qui donne k équations ;

ii) $P(x) = G(x)$ pour chaque $x \in X' \setminus (X_1 \cup X_2)$, ce qui donne $q - 2k$ équations additionnelles ;

iii) $P(z) = \Pi(F^{-1}(z))$ pour chaque $z \in X_2$ (remarquons que $X_2 \subseteq S$), de sorte que $P(P(x)) = \Pi(x)$ pour chaque $x \in X_1$; cela donne k équations additionnelles ;

iv) $P(z) = \Pi(F(\Pi^{-1}(z)))$ pour chaque $z \in Y_1$ (remarquons que $Y_1 \subseteq S$), de sorte que $P(P(x)) = \Pi(x)$ pour chaque $x \in X_2$; cela donne k équations additionnelles puisque $Y_1 \cap X' = \emptyset$;

v) $P(z) = \Pi(G^{-1}(z))$ pour chaque $z \in W$, de sorte que $P(P(x)) = \Pi(x)$ pour chaque $x \in X' \setminus (X_1 \cup X_2)$; cela donne $q - 2k$ équations additionnelles puisque W est disjoint de $X' \cup Y_1$.

Au total, cela donne $(2q - k)$ équations, ce qui prouve (6.22). En combinant (6.20), (6.21), et (6.22), et puisque $q'' \geq q - 4\lfloor M \rfloor$, on a

$$\begin{aligned}
\mathsf{p}^* &\geq \sum_{0 \leq k \leq M} \frac{(q'')_{2k}(N - 2q - 2q')_{q-2k}}{k!(N - q')_{2q-k}} \\
&\geq \sum_{0 \leq k \leq M} \frac{(q)_{2k}(N - 2q - q')_{q-2k}(N - q')_q}{k!(N - q')_{2q-k}} \times \frac{(q - 4\lfloor M \rfloor)_{2k}(N - 2q - 2q')_{q-2k}}{(q)_{2k}(N - 2q - q')_{q-2k}(N - q')_q} \\
&\geq \frac{1}{(N)_q} \sum_{0 \leq k \leq M} C_{N-q',q,k} \times \underbrace{\frac{(q - 4\lfloor M \rfloor)_{2k}}{(q)_{2k}}}_{A} \times \underbrace{\frac{(N)_q(N - 2q - 2q')_{q-2k}}{(N - q')_q(N - 2q - q')_{q-2k}}}_{B}\,,
\end{aligned}$$

où la variable $C_{N,q,k}$ a été définie au lemme 6.4, section 6.2.5. De plus, pour tout $0 \leq k \leq M$, on a

$$A \geq \frac{(q-4\lfloor M\rfloor)_{2\lfloor M\rfloor}}{(q)_{2\lfloor M\rfloor}} \geq \left(1-\frac{4\lfloor M\rfloor}{q-2\lfloor M\rfloor+1}\right)^{2\lfloor M\rfloor} \geq 1-\frac{8\lfloor M\rfloor^2}{q-2\lfloor M\rfloor+1} \geq 1-\frac{12\lfloor M\rfloor^2}{q},$$

où, pour la dernière inégalité, on utilise l'hypothèse (A.2) qui implique que $q-2\lfloor M\rfloor \geq 2q/3$, et

$$B \geq \frac{(N)_q(N-2q-2q')_q}{(N-q')_q(N-2q-q')_q} \geq 1-\frac{4q(q+q')^2}{N^2},$$

où on applique le lemme 6.3 avec $a=q$, $b=q+q'$, $c=q'$, et $d=2q+q'$ (remarquons que $2a+2b \leq N$ par l'hypothèse (A.3)).

Ainsi, on obtient finalement, en utilisant le lemme 6.4 (remarquons que la condition $M \leq q/2 \leq (N-q')/6$ nécessaire pour appliquer le lemme 6.4 est déduite des hypothèses (A.2) et (A.3)),

$$\begin{aligned}\mathsf{p}^* &\geq \frac{1}{(N)_q}\left(1-\frac{2M^2}{q}-\frac{3q^2}{2M(N-q')}-\frac{12M^2}{q}-\frac{4q(q+q')^2}{N^2}\right)\\ &\geq \frac{1}{(N)_q}\left(1-\frac{14M^2}{q}-\frac{3q^2}{MN}-\frac{4q(q+q')^2}{N^2}\right),\end{aligned}$$

où la dernière inégalité provient de l'hypothèse (A.3) qui implique que $N-q' \geq N/2$. ∎

6.6.2 Probabilité d'une mauvaise transcription pour des clés de tours non indépendantes

Dans cette section, on se concentre sur le cas où $\ell = n$, c'est-à-dire le cas où la clé principale k est de la même taille que la taille des blocs (et donc de la même taille que les clés de tours). On traite des cas plus simples où les trois clés sont indépendantes, ou dérivées de deux clés indépendantes de n bits, respectivement en section 6.7 et en section 6.8. Tout d'abord, on décrit les propriétés de $\boldsymbol{\gamma} = (\gamma_0, \gamma_1, \gamma_2)$ pour pouvoir majorer efficacement la probabilité d'obtenir une mauvaise transcription (dans le monde idéal).

Définition 6.3
On dit que les fonctions de dérivations $\boldsymbol{\gamma} = (\gamma_0, \gamma_1, \gamma_2)$, où $\gamma_i : \{0,1\}^n \to \{0,1\}^n$, sont *bonnes* si elles vérifient les conditions suivantes :

(i) $\gamma_0, \gamma_1, \gamma_2 \in \mathsf{GL}(n)$ (chaque γ_i est une bijection linéaire sur $\mathbb{F}_2^n$) ;

(ii) $\gamma_0 \oplus \gamma_1 \in \mathsf{GL}(n)$ et $\gamma_1 \oplus \gamma_2 \in \mathsf{GL}(n)$;

(iii) $\gamma_0 \oplus \gamma_1 \oplus \gamma_2$ est une permutation sur $\{0,1\}^n$ (non nécessairement linéaire sur $\mathbb{F}_2^n$). ♦

Une manière simple de construire un tel uplet $(\gamma_0, \gamma_1, \gamma_2)$ est de prendre $\gamma_0 = \gamma_2 = Id$ l'identité, et $\gamma_1 = \pi$, où π est un orthomorphisme linéaire de $\mathbb{F}_2^n$ (on rappelle qu'une permutation π de $\{0,1\}^n$ est un orthomorphisme si $x \mapsto x \oplus \pi(x)$ est aussi une permutation), de sorte que la suite de clés de tours est $(k, \pi(k), k)$. Nous donnons deux exemples simples d'orthomorphismes linéaires qui sont intéressants du point de vue de l'implémentation :

– Quand n est pair et $k = (k_L, k_R)$, où k_L et k_R sont respectivement les moitiés gauche et droite de k, alors
$$\pi : (k_L, k_R) \mapsto (k_R, k_L \oplus k_R)$$
est un orthomorphisme linéaire.
– Fixons un polynôme irréductible p de degré n sur $\mathbb{F}_2$ et on identifie $\mathbb{F}_2^n$ et le corps $\mathbb{F}_{2^n}$ defini par p de manière canonique. Alors, pour tout $c \in \mathbb{F}_{2^n} \setminus \{0, 1\}$, $k \mapsto c \odot k$ (où $\odot$ est la multiplication dans le corps $\mathbb{F}_{2^n}$) est un orthomorphisme linéaire.

Lemme 6.16. *Soit $\boldsymbol{\gamma} = (\gamma_0, \gamma_1, \gamma_2)$ des bonnes fonctions de dérivation. Supposons que $9n \le q_e, q_p \le N/2$. Alors*
$$\Pr[T_{\mathrm{id}} \in \mathcal{T}_2] \le \frac{10}{N} + \frac{4q_e^2 q_p + 7q_e q_p^2 + 4q_p^2\sqrt{q_e q_p}}{N^2} + \frac{9q_p\sqrt{nq_e} + 6q_e\sqrt{nq_p}}{N} + \frac{q_e + 12q_p}{N^{\frac{2}{3}}}\,. \qquad \triangledown$$

Démonstration. Dans le monde idéal, les ensembles BadK_i ne dépendent que des permutations aléatoires E et P, et pas de la clé k qui est tirée uniformément aléatoire à la fin de l'interaction du distingueur avec (E, P). De plus, la taille de BadK_i, pour $i = 6$ jusqu'à 10, peut être majorée indépendamment de E, P. En effet, puisque γ_0, γ_2, $\gamma_0 \oplus \gamma_1$, $\gamma_1 \oplus \gamma_2$, et $\gamma_0 \oplus \gamma_1 \oplus \gamma_2$ sont toutes des permutations de $\{0,1\}^n$, on a, pour toute transcription de permutations $(\mathcal{Q}_E, \mathcal{Q}_P)$,
$$|\mathsf{BadK}_6|, |\mathsf{BadK}_7|, |\mathsf{BadK}_8|, |\mathsf{BadK}_9| \le \frac{3q_e q_p}{M}\,,$$
$$|\mathsf{BadK}_{10}| \le \frac{q_e^2}{M}\,,$$
de sorte que
$$\Pr\left[k \leftarrow_{\$} \{0,1\}^n : k \in \bigcup_{i=6}^{10} \mathsf{BadK}_i\right] \le \frac{12q_e q_p}{NM} + \frac{q_e^2}{NM} \le \frac{q_e + 12q_p}{N^{\frac{2}{3}}}\,.$$

Pour majorer $|\mathsf{BadK}_i|$, pour $i = 1$ jusqu'à 5, on utilise le théorème « sum-capture » de la section 6.3. Pour une transcription de permutations $(\mathcal{Q}_E, \mathcal{Q}_P)$, soit
$$X = \{x \in \{0,1\}^n : (x, y) \in \mathcal{Q}_E\}, \qquad Y = \{y \in \{0,1\}^n : (x, y) \in \mathcal{Q}_E\},$$
$$U = \{u \in \{0,1\}^n : (u, v) \in \mathcal{Q}_P\}, \qquad V = \{v \in \{0,1\}^n : (u, v) \in \mathcal{Q}_P\}$$
les domaines et les images de $\mathcal{Q}_E$ et $\mathcal{Q}_P$, respectivement. Alors
$$|\mathsf{BadK}_1| \le \mu(\mathcal{Q}_E, U, V) \stackrel{\text{def}}{=} |\{((x, y), u, v) \in \mathcal{Q}_E \times U \times V : x \oplus u = \gamma_0 \circ \gamma_2^{-1}(y \oplus v)\}|$$
$$|\mathsf{BadK}_2| \le \mu(\mathcal{Q}_P, X, U) \stackrel{\text{def}}{=} |\{((u, v), x, u') \in \mathcal{Q}_P \times X \times U : x \oplus u = \gamma_0 \circ \gamma_1^{-1}(v \oplus u')\}|$$
$$|\mathsf{BadK}_3| \le \mu(\mathcal{Q}_P, V, Y) \stackrel{\text{def}}{=} |\{((u', v'), v, y) \in \mathcal{Q}_P \times V \times Y : v \oplus u' = \gamma_1 \circ \gamma_2^{-1}(v' \oplus y)\}|$$
$$|\mathsf{BadK}_4| \le \mu(\mathcal{Q}_P, X, X) \stackrel{\text{def}}{=} |\{((u, v), x, x') \in \mathcal{Q}_P \times X \times X : x \oplus u = \gamma_0 \circ (\gamma_0 \oplus \gamma_1)^{-1}(v \oplus x')\}|$$
$$|\mathsf{BadK}_5| \le \mu(\mathcal{Q}_P, Y, Y) \stackrel{\text{def}}{=} |\{((u, v), y, y') \in \mathcal{Q}_P \times Y \times Y : y' \oplus u = (\gamma_1 \oplus \gamma_2) \circ \gamma_2^{-1}(v \oplus y)\}|\,.$$

Puisque les fonctions de dérivations sont bonnes, on a que $\gamma_0 \circ \gamma_2^{-1}$, $\gamma_0 \circ \gamma_1^{-1}$, $\gamma_1 \circ \gamma_2^{-1}$, $\gamma_0 \circ (\gamma_0 \oplus \gamma_1)^{-1}$, et $\gamma_0 \circ (\gamma_0 \oplus \gamma_1)^{-1}$ sont tous des automorphismes de $\mathbb{F}_2^n$. Ainsi, on peut

appliquer le théorème 6.5 (remarquons que, pour appliquer ce théorème pour majorer, disons, $|\mathsf{BadK}_1|$, on considère la combinaison du distingueur $\mathcal{D}$ et de la permutation P comme un adversaire probabiliste $\mathcal{A}$ interagissant avec la permutation E, produisant la transcription $\mathcal{Q}_E$). Ainsi, si on fixe

$$\begin{aligned} C_1 &= \frac{q_e q_p^2}{N} + \frac{2q_e^2 q_p}{N} + 3q_p\sqrt{nq_e} \\ C_2 = C_3 &= \frac{q_e q_p^2}{N} + \frac{2q_p^2\sqrt{q_e q_p}}{N} + 3q_p\sqrt{nq_e} \\ C_4 = C_5 &= \frac{q_e^2 q_p}{N} + \frac{2q_e q_p^2}{N} + 3q_e\sqrt{nq_p}\,, \end{aligned}$$

on a $\Pr[E, P \leftarrow_\$ \mathcal{P}_n : |\mathsf{BadK}_i| \geq C_i] \leq 2/N$ pour chaque $i = 1$ jusqu'à 5. Puisque

$$\Pr[T_{\mathrm{id}} \in \mathcal{T}_2] \leq \sum_{i=1}^{5} \Pr[E, P \leftarrow_\$ \mathcal{P}_n : |\mathsf{BadK}_i| \geq C_i] + \frac{\sum_{i=1}^{5} C_i}{N} + \frac{q_e + 12q_p}{N^{\frac{2}{3}}}\,,$$

on obtient bien le résultat voulu.

En combinant les lemmes 6.1, 6.14, et 6.16, on obtient le théorème principal de ce chapitre.

Théorème 6.17 (Une seule permutation et des clés de tours non-indépendantes). *On considère le schéma d'Even-Mansour généralisé à deux tours et une permutation* $\mathsf{EMSP}[n, 2, \boldsymbol{\gamma}]$ *avec de bonnes fonctions de dérivations* $\boldsymbol{\gamma}$ *(voir définition 6.3). Supposons que* $N \geq 7^3$, $9n \leq q_e, q_p \leq N/2$, *et* $4q_e + 2q_p \leq N$. *Alors*

$$\begin{aligned} \mathbf{Adv}^{\mathrm{cca}}_{\mathsf{EMSP}[n,2,\gamma]}(q_e, q_p) \leq \frac{10}{N} + \frac{4q_e^3 + 12q_e^2 q_p + 11q_e q_p^2 + 4q_p^2\sqrt{q_e q_p}}{N^2} + \frac{2q_e^2}{N^{\frac{4}{3}}} \\ + \frac{9q_p\sqrt{nq_e} + 6q_e\sqrt{nq_p}}{N} + \frac{21q_e + 12q_p}{N^{\frac{2}{3}}}\,. \quad \diamondsuit \end{aligned}$$

En posant $q = \max(q_e, q_p)$, et en supposons que $q \leq N^{\frac{2}{3}}$, la majoration du théorème 6.17 se simplifie en

$$\frac{10}{N} + \frac{31q^3}{N^2} + \frac{2q^2}{N^{\frac{4}{3}}} + \frac{15\sqrt{n}q^{\frac{3}{2}}}{N} + \frac{33q}{N^{\frac{2}{3}}} \leq \frac{10}{N} + \frac{81\sqrt{n}q}{N^{\frac{2}{3}}} = \frac{10}{2^n} + \frac{81q}{2^{\frac{2n}{3} - \frac{1}{2}\log_2 n}}\,.$$

Ainsi, la sécurité du schéma est assurée jusqu'à $\mathcal{O}(2^{\frac{2n}{3} - \frac{1}{2}\log_2 n}) = \widetilde{\mathcal{O}}(2^{\frac{2n}{3}})$ requêtes de l'adversaire.

6.7 Probabilité d'une mauvaise transcription pour trois clés de tours indépendantes

Dans cette section, on majore la probabilité d'obtenir une mauvaise transcription pour le schéma d'Even-Mansour généralisé à deux tours à une permutation et pour des clés de tours (k_0, k_1, k_2) indépendantes, c'est-à-dire $\ell = 3n$, $K = (k_0, k_1, k_2)$, et γ_i sélectionne la i-ème chaîne de n bits de K. L'analyse est alors grandement simplifiée car nous n'avons pas besoin d'utiliser le théorème « sum-capture » de la section 6.3.

Lemme 6.18. *Supposons que les clés de tours (k_0, k_1, k_2), dans le schéma d'Even-Mansour généralisé à deux tours à une permutation, soient indépendantes. Alors*

$$\Pr[T_{\mathrm{id}} \in \mathcal{T}_2] \leq \frac{2q_e^2 q_p + 3q_e q_p^2}{N^2} + \frac{q_e + 12q_p}{N^{\frac{2}{3}}}\,. \qquad \triangledown$$

Démonstration. Soit $(\mathcal{Q}_E, \mathcal{Q}_P)$ une transcription (de permutations) atteignable. Puisque, dans le monde idéal, $K = (k_0, k_1, k_2)$ est indépendante de $\mathcal{Q}_E$ et $\mathcal{Q}_P$, on a

$$\Pr[K = (k_0, k_1, k_2) \leftarrow_{\$} \{0,1\}^{3n} : K \in \mathsf{BadK}] \leq \frac{|\mathsf{BadK}|}{N^3}\,.$$

Remarquons que, pour toute transcription de permutations $(\mathcal{Q}_E, \mathcal{Q}_P)$, on a

$$\begin{aligned} |\mathsf{BadK}_1|, |\mathsf{BadK}_2|, |\mathsf{BadK}_3| &\leq N q_e q_p^2\,, \\ |\mathsf{BadK}_4|, |\mathsf{BadK}_5| &\leq N q_e^2 q_p\,, \\ |\mathsf{BadK}_6|, |\mathsf{BadK}_7|, |\mathsf{BadK}_8|, |\mathsf{BadK}_9| &\leq \frac{3N^2 q_e q_p}{M}\,, \\ |\mathsf{BadK}_{10}| &\leq \frac{N^2 q_e^2}{M}\,. \end{aligned}$$

Le résultat s'en déduit en utilisant $M = q_e/N^{1/3}$. ∎

En combinant les lemmes 6.1, 6.14, et 6.18, on obtient le théorème suivant qui implique une sécurité jusqu'à $\mathcal{O}(2^{2n/3})$ requêtes.

Théorème 6.19 (Une permutation et des clés de tours indépendantes). *Soit $\boldsymbol{\gamma} = (\gamma_0, \gamma_1, \gamma_2)$, où $\gamma_i : (k_0, k_1, k_2) \mapsto k_i$. Considérons le schéma d'Even-Mansour généralisé à deux tours, à une permutation et pour des clés de tours (k_0, k_1, k_2) indépendantes $\mathsf{EMSP}[n, 2, \ell = 3n, \boldsymbol{\gamma}]$. Supposons que $N \geq 7^3$ et $4q_e + 2q_p \leq N$. Alors*

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{EMSP}[n,2,3n,\boldsymbol{\gamma}]} \leq \frac{4q_e^3 + 10q_e^2 q_p + 7q_e q_p^2}{N^2} + \frac{2q_e^2}{N^{\frac{4}{3}}} + \frac{21q_e + 12q_p}{N^{\frac{2}{3}}}. \qquad \diamondsuit$$

6.8 Probabilité d'une mauvaise transcription pour deux clés de tours indépendantes

On considère dans cette section le cas d'une clé principale K de longueur $2n$, à savoir $K = (k, k')$, et les clés de tours sont (k, k', k). Ce cas est intéressant car il s'agit de l'analogue pour deux tours du processus de dérivation des clés du schéma LED-128 [GPPR11] (qui a 12 tours), où la clé principale $K = (k, k')$ est deux fois plus longue que la taille des blocs, et les clés de tours k et k' sont xorés alternativement à l'état. Cette configuration est intermédiaire entre le cas de clés de tours indépendantes et le cas d'une clé principale à n bits. En particulier, le théorème sum-capture est nécessaire uniquement pour majorer $|\mathsf{BadK}_1|$.

Lemme 6.20. *Considérons le schéma d'Even-Mansour généralisé à deux tours, à une permutation et avec comme clé principale $K = (k, k')$ et clés de tours (k, k', k), k et k' étant uniformément aléatoires et indépendantes. Supposons que $9n \leq q_e, q_p \leq N/2$. Alors*

$$\Pr[T_{\mathrm{id}} \in \mathcal{T}_2] \leq \frac{2}{N} + \frac{4q_e^2 q_p + 3q_e q_p^2}{N^2} + \frac{3q_p\sqrt{nq_e}}{N} + \frac{q_e + 12q_p}{N^{\frac{2}{3}}}. \qquad \triangledown$$

Démonstration. Dans le monde idéal, les ensembles BadK_i dépendent uniquement des permutations aléatoires E et P, et pas de la clé $K = (k, k')$ qui est tirée uniformément aléatoire à la fin de l'interaction du distingueur avec (E, P). De plus, la taille de BadK_i, pour $i = 2$ jusqu'à 10, peut être majorée indépendamment de E, P, à savoir que, pour toute transcription de permutations $(\mathcal{Q}_E, \mathcal{Q}_P)$, on a

$$\begin{aligned} |\mathsf{BadK}_2|, |\mathsf{BadK}_3| &\leq q_e q_p^2, \\ |\mathsf{BadK}_4|, |\mathsf{BadK}_5| &\leq q_e^2 q_p, \\ |\mathsf{BadK}_6|, |\mathsf{BadK}_7|, |\mathsf{BadK}_8|, |\mathsf{BadK}_9| &\leq \frac{3Nq_e q_p}{M}, \\ |\mathsf{BadK}_{10}| &\leq \frac{Nq_e^2}{M}, \end{aligned}$$

de sorte que

$$\begin{aligned} \Pr\left[(k, k') \leftarrow_{\$} \{0,1\}^{2n} : (k, k') \in \bigcup_{i=2}^{10} \mathsf{BadK}_i\right] &\leq \frac{2q_e q_p^2 + 2q_e^2 q_p}{N^2} + \frac{12q_e q_p}{NM} + \frac{q_e^2}{NM} \\ &\leq \frac{2q_e q_p^2 + 2q_e^2 q_p}{N^2} + \frac{q_e + 12q_p}{N^{\frac{2}{3}}}. \end{aligned}$$

Il reste à majorer $|\mathsf{BadK}_1|$. Pour cela, on utilise le théorème sum-capture de la section 6.3. Pour une transcription de permutations $(\mathcal{Q}_E, \mathcal{Q}_P)$, soient

$$\begin{aligned} X &= \{x \in \{0,1\}^n : (x, y) \in \mathcal{Q}_E\}, & Y &= \{y \in \{0,1\}^n : (x, y) \in \mathcal{Q}_E\}, \\ U &= \{u \in \{0,1\}^n : (u, v) \in \mathcal{Q}_P\}, & V &= \{v \in \{0,1\}^n : (u, v) \in \mathcal{Q}_P\} \end{aligned}$$

les domaines et images de $\mathcal{Q}_E$ et $\mathcal{Q}_P$, respectivement. Alors

$$|\mathsf{BadK}_1| \leq \mu(\mathcal{Q}_E, U, V) \stackrel{\text{def}}{=} |\{((x, y), u, v) \in \mathcal{Q}_E \times U \times V : x \oplus u = y \oplus v\}|.$$

Et, si on pose

$$C_1 = \frac{q_e q_p^2}{N} + \frac{2q_e^2 q_p}{N} + 3q_p\sqrt{nq_e},$$

on a, par le théorème 6.5, $\Pr[E, P \leftarrow_{\$} \mathcal{P}_n : |\mathsf{BadK}_1| \geq C_1] \leq 2/N$. Ainsi, on obtient

$$\begin{aligned} \Pr[T_{\mathrm{id}} \in \mathcal{T}_2] &\leq \Pr[E, P \leftarrow_{\$} \mathcal{P}_n : |\mathsf{BadK}_1| \geq C_1] + \frac{C_1}{N} \\ &\qquad + \Pr\left[(k, k') \leftarrow_{\$} \{0,1\}^{2n} : (k, k') \in \bigcup_{i=2}^{10} \mathsf{BadK}_i\right] \\ &\leq \frac{2}{N} + \frac{q_e q_p^2}{N^2} + \frac{2q_e^2 q_p}{N^2} + \frac{3q_p\sqrt{nq_e}}{N} + \frac{2q_e q_p^2 + 2q_e^2 q_p}{N^2} + \frac{q_e + 12q_p}{N^{\frac{2}{3}}} \\ &= \frac{2}{N} + \frac{4q_e^2 q_p + 3q_e q_p^2}{N^2} + \frac{3q_p\sqrt{nq_e}}{N} + \frac{q_e + 12q_p}{N^{\frac{2}{3}}}. \end{aligned}$$

■

En combinant les lemmes 6.1, 6.14, et 6.20, on obtient le théorème suivant qui implique une sécurité jusqu'à $\widetilde{\mathcal{O}}(2^{2n/3})$ requêtes.

Théorème 6.21 (Une permutation et deux clés de tours alternées et indépendantes). *Soit $\boldsymbol{\gamma} = (\gamma_0, \gamma_1, \gamma_2)$, où $\gamma_i : (k_0, k_1) \mapsto k_{i \bmod 2}$. Considérons le schéma d'Even-Mansour généralisé à deux tours $\mathsf{EMSP}[n, 2, \ell = 2n, \boldsymbol{\gamma}]$, à une permutation et avec comme clé principale $K = (k, k')$ et clés de tours (k, k', k), k et k' étant uniformément aléatoires et indépendantes. Supposons que $N \geq 7^3$, $9n \leq q_e, q_p \leq N/2$, et $4q_e + 2q_p \leq N$. Alors*

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{EMSP}[n,2,2n,\boldsymbol{\gamma}]} \leq \frac{2}{N} + \frac{4q_e^3 + 12q_e^2 q_p + 7q_e q_p^2}{N^2} + \frac{2q_e^2}{N^{\frac{4}{3}}} + \frac{3q_p\sqrt{nq_e}}{N} + \frac{21q_e + 12q_p}{N^{\frac{2}{3}}}. \qquad \diamondsuit$$

Chapitre 7

Les différentes techniques de preuve d'indistinguabilité dans les modèles idéalisés

Au cours des chapitres précédents, nous avons vu différentes techniques pour prouver l'indistinguabilité de certains schémas idéalisés, comme le schéma d'Even-Mansour itéré pour lequel les permutations internes sont uniformément aléatoires, la version idéalisée du schéma CLRW où l'on remplace les appels au schéma E par des appels à des permutations uniformément aléatoires, les KAF où l'on considère des fonctions internes uniformément aléatoires. Le coupling nous a permis d'établir des bornes de sécurité pour un nombre arbitraire de tours mais les résultats par coupling n'ont pas donné de preuves optimales. A l'inverse, les preuves « classiques » utilisant la technique des jeux permettent en général d'obtenir des résultats optimaux mais qui sont difficilement généralisables à un nombre arbitraire de tours. La technique des coefficients H inventée par Jacques Patarin [Pat91, Pat08] permet, elle, de prouver des résultats optimaux pour un nombre arbitraire de tours dans certains cas, comme l'ont montré [CS14] dans leur preuve optimale du schéma d'Even-Mansour itéré. On peut également noter les résultats de la théorie des systèmes aléatoires de Maurer [Mau02, MP03, MP04, MPR07], qui unifie la façon de traiter les différentes primitives cryptographiques et leurs preuves de sécurité. Toutes ces techniques ont leur qualités et leur défauts et, lors de cette thèse, nous avons exploré ces différentes techniques pour les combiner ou s'en inspirer dans nos preuves. Ce chapitre présente et compare les principales techniques employées pour prouver l'indistinguabilité dans les modèles idéalisés.

7.1 Les jeux

La technique de preuve d'indistinguabilité par jeux est la technique la plus utilisée et l'une des plus efficaces. Elle est pour la première fois formalisée en 1994 par Kilian et Rogaway [KR96] puis très largement utilisée par Rogaway et ses coauteurs [BKR98, BRW04, BR00, BR02, BRS02, HR04, HR03, Rog02, Rog04, RBBK01], Shoup [AGKS05, CS03a, CS03b, CS02, SS00, Sho01, Sho00] et d'autres auteurs.

Elle a de nombreux avantages et quelques inconvénients que nous allons décrire en sections 7.1.2 et 7.1.3. Elle est notamment facile d'emploi, applicable très largement (dans

des modèles idéalisés ou non) et, appliquée de la bonne manière, elle permet des preuves simples et très intuitives. En revanche, jusqu'à maintenant, cette technique semble être difficile à utiliser pour des schémas ayant un nombre élevé de tours.

En quoi consiste cette technique ? Imaginons un attaquant $\mathcal{A}$ qui souhaite distinguer une construction cryptographique (dans un monde dit réel) d'une construction idéale (dans un monde dit idéal). On sait que, par définition, l'avantage pour distinguer ces deux mondes est égal à la différence entre la probabilité que l'attaquant réponde 1 dans le monde réel et la probabilité qu'il réponde 1 dans le monde idéal. Il est possible de représenter le comportement de l'attaquant dans un monde donné par un programme qu'on appelle « jeu ». Si « jeu 0 » et « jeu 1 » sont les jeux respectifs pour le monde réel et le monde idéal, il s'agit de définir un événement bad dans les deux jeux, initialisé à false, tel que ceux-ci soient syntaxiquement identiques tant que bad vaut false. Alors, le « lemme fondamental des jeux » établit que l'avantage de l'attaquant est majoré par la probabilité de déclencher l'événement bad.

7.1.1 Exemple

Pour mieux comprendre cette technique, nous présentons un exemple très simple qui consiste à étudier l'indistinguabilité entre une permutation uniformément aléatoire π et une fonction uniformément aléatoire f. Nous allons prouver le lemme suivant :

Lemme 7.1. *Soient q et n des entiers positifs, π une permutation uniformément aléatoire de $\mathcal{P}_n$ et f une fonction uniformément aléatoire de $\mathcal{F}_n$. Pour tout adversaire $\mathcal{A}$ faisant au plus q requêtes, on a*

$$\left|\Pr\left[\mathcal{A}^{\pi} \Rightarrow 1\right] - \Pr\left[\mathcal{A}^{f} \Rightarrow 1\right]\right| \leq \frac{q(q-1)}{2^{n+1}} \quad . \qquad \triangledown$$

Jeux J1

1: **Procedure** P(x)
2: $y \leftarrow_{\$} \{0,1\}^n$
3: **if** $y \in image(p)$ **then**
4: bad $\leftarrow$ true
5:
6:
7: **return** $p(x) \leftarrow y$

Jeux J2

1: **Procedure** P(x)
2: $y \leftarrow_{\$} \{0,1\}^n$
3: **if** $y \in image(p)$ **then**
4: bad $\leftarrow$ true
5: **if** bad = true **then**
6: $y \leftarrow_{\$} \overline{image}(p)$
return $p(x) \leftarrow y$

FIGURE 7.1 – Jeux J1 et J2 simulant respectivement une fonction uniformément aléatoire et une permutation uniformément aléatoire.

Supposons, sans perte de généralité, que l'attaquant est déterministe et ne fait jamais de requêtes redondantes. Plutôt que de considérer $\mathcal{A}$ interagissant avec π ou f, on imagine $\mathcal{A}$ interagissant avec le jeu J1 ou le jeu J2 présentés en figure 7.1. Chaque jeu rend accessible à l'attaquant un oracle P et l'attaquant peut effectuer des requêtes du type $P(x)$, la valeur retournée étant la valeur calculée en exécutant le code du jeu. Par convention, on considère que bad est initialisé à false et p est un tableau dont les valeurs sont initialement non

définies. L'ensemble $image(p)$ est l'ensemble des y tels qu'il existe x vérifiant $p[x] = y$. L'ensemble $\overline{image}(p)$ est le complémentaire de $image(p)$. A chaque réponse de l'oracle P, le jeu met à jour le tableau p.

Soit $\mathcal{A}^J \Rightarrow 1$ l'événement « $\mathcal{A}$ répond 1 dans le jeu J », pour $J \in \{J1, J2\}$. On remarque tout d'abord que les jeux J1 et J2 simulent parfaitement le comportement d'une fonction uniformément aléatoire et d'une permutation uniformément aléatoire respectivement. Ainsi, l'avantage de l'attaquant pour distinguer J1 de J2 est identique à son avantage pour distinguer une permutation uniformément aléatoire π d'une fonction uniformément aléatoire f, c'est-à-dire

$$\left|\Pr\left[\mathcal{A}^{\pi} \Rightarrow 1\right] - \Pr\left[\mathcal{A}^{f} \Rightarrow 1\right]\right| = \left|\Pr\left[\mathcal{A}^{J2} \Rightarrow 1\right] - \Pr\left[\mathcal{A}^{J1} \Rightarrow 1\right]\right| \ .$$

Puisque les jeux sont syntaxiquement identiques tant que bad reste false, on a

$$\left|\Pr\left[\mathcal{A}^{J2} \Rightarrow 1\right] - \Pr\left[\mathcal{A}^{J1} \Rightarrow 1\right]\right| \leq \Pr\left[\mathsf{bad}\right] \ .$$

Cette inégalité provient du « lemme fondamental des jeux » que nous ne prouverons pas ici (voir [BR06]). Il s'agit maintenant de majorer la probabilité de l'événement bad. On remarque facilement que $y \in image(p)$ avec probabilité $\frac{\ell}{2^n}$ lors de la $\ell + 1$-ème requête à P. Ainsi, par la borne de l'union, on a

$$\Pr\left[\mathsf{bad}\right] \leq \sum_{\ell=1}^{q-1} \frac{\ell}{2^n} = \frac{q(q-1)}{2^{n+1}} \ ,$$

ce qui permet de conclure.

7.1.2 Avantages

Pourquoi la technique de preuve par jeux est-elle la plus répandue ?

Application large

Les preuves par jeux peuvent s'appliquer à toute construction cryptographique, contrairement aux techniques par coupling ou par coefficients H qui se sont, jusqu'à maintenant, limitées aux preuves d'indistinguabilité par rapport à une permutation aléatoire ou à une fonction aléatoire. Elles sont applicables et formulables non seulement aux modèles idéalisés mais aussi au modèle standard, où les éléments idéaux sont instanciés, contrairement aux autres techniques. Par exemple, au chapitre 4, nous n'avons introduit la technique du coupling qu'après avoir utilisé un argument hybride pour idéaliser les éléments internes. Avec la technique des jeux, il est possible de partir directement du système instancié, en le considérant comme un jeu, puis introduire un jeu intermédiaire avec les éléments internes idéalisés, et considérer un jeu final « idéal » (comme une permutation ou une fonction uniformément aléatoire).

Simple et intuitif la plupart du temps

Comme nous l'avons vu dans l'exemple précédent, pour des schémas simples, cette technique est très intuitive au sens où il n'y pas de calculs « artificiels » (comme pour la technique des coefficients H) pour obtenir une majoration de l'avantage. Dans les cas simples, les calculs sont intrinsèquement liés à la différence entre les deux schémas. Dans l'exemple précédent, le calcul de la probabilité des collisions correspond exactement à la différence structurelle entre les deux schémas.

Une rigueur importante

Les preuves par jeux font preuve d'une grande rigueur au sens où, si l'on voit une preuve comme une succession de pas logiques plus ou moins faciles à vérifier/accepter intellectuellement, chaque pas est suffisamment petit pour s'assurer de la validité de chaque étape. Contrairement à certaines techniques, par exemple pour les systèmes aléatoires, où il peut être un peu plus facile de se laisser piéger par une preuve trop rapide (voir par exemple [JÖS12]).

On peut dire que c'est le cumul de ces qualités qui a rendu les preuves par jeux si pratiques et si utilisées.

7.1.3 Inconvénients

Malheureusement, cette technique possède quelques faiblesses et c'est pour cela qu'il a récemment fallu utiliser d'autres techniques là où les jeux semblent impuissants.

Une complexité fortement liée au nombre de tours

Dans le cas de l'étude de schémas avec un nombre arbitraire de tours, les preuves par jeux s'en sortent très mal. Par exemple, pour le schéma d'Even-Mansour, les premières preuves pour 2 et 3 tours (par [BKL$^+$12] et [Ste12]) sont longues, compliquées et, surtout, des preuves pour 4 tours et plus semblent inatteignables avec cette technique. Pour le cas du schéma CLRW, on remarque que les travaux de Landecker, Shrimpton et Terashima [LST12], qui donnent une preuve par jeux pour le schéma CLRW à 2 tours, est déjà très complexe. D'autre part, comme pour le schéma d'Even-Mansour, la complexité de la preuve semble exponentielle en le nombre de tours. Ainsi, de la même manière, une preuve pour 3 ou 4 tours semble très complexe avec cette technique, contrairement aux preuves par coupling par exemple.

Une complexité parfois artificielle

Pour le schéma CLRW à 2 tours, la preuve citée de Landecker, Shrimpton et Terashima [LST12] utilise 7 jeux différents et la partie essentielle de la preuve (le calcul de la probabilité de certaines collisions) semble « noyée » par d'autres considérations artificielles. C'est également le cas pour d'autres preuves comme la preuve de sécurité par jeux du CBC MAC de Bellare, Kilian et Rogaway [BKR00] et la plupart des preuves par jeux qui nécessitent un nombre arbitraire d'itérations. Cette complexité des preuves par jeux, et notamment pour le schéma CBC, est relatée dans l'article de Bernstein [Ber05] qui propose une preuve très simple du schéma CBC (qui utilise exactement la technique des coefficients H, sans la nommer) et critique la complexité artificielle de certaines preuves par jeux.

7.2 Les coefficients H (Patarin)

Nous avons décrit et utilisé la technique des coefficients H [Pat91, Pat08] à de nombreuses reprises (en particulier en sections 2.6, 3.5.1, 4.4 et 6.2.4). Cette technique consiste à transposer le problème cryptographique en un problème purement combinatoire. Étant donné un schéma de chiffrement par blocs $E \in \mathsf{BC}(\mathcal{K}, \mathcal{D})$, un des théorèmes principaux de la théorie des coefficients H établit que :

Théorème 7.2. *Si il existe $\alpha > 0$, $\beta > 0$ et Ω un sous-ensemble de $\mathcal{D}^q$ vérifiant $|\Omega| \geq (1-\beta)|\mathcal{D}^q|$ tel que, pour tout $x = (x_1, \ldots, x_q) \in \mathcal{D}^q$ où les x_i sont deux à deux distincts et pour tout $y = (y_1, \ldots, y_q) \in \Omega$, on a :*

$$\Pr\left[k \leftarrow_{\$} \mathcal{K} : E_k(x) = y\right] \geq (1-\alpha) \Pr\left[f \leftarrow_{\$} \mathcal{F}_n : f(x) = y\right] \ ,$$

où $E_k(x) = y$ (et $f(x) = y$) signifient que $E_k(x_i) = y_i$ pour tout $i \leq q$ (respectivement $f(x_i) = y_i$ pour tout $i \leq q$), alors l'avantage (adaptatif) pour distinguer le schéma E d'une fonction uniformément aléatoire f est majoré par $\alpha + \beta$. ♢

Intuitivement, ce théorème dit que, si pour presque tous les uplets d'entrées/sorties, la probabilité que les entrées soient envoyées sur les sorties par E est proche de la probabilité que les entrées soient envoyées sur les sorties par une fonction uniformément aléatoire f, alors E est indistinguable d'une fonction uniformément aléatoire.

Notons qu'il y a de nombreuses variantes de ce théorème, par exemple pour comparer un schéma avec une permutation uniformément aléatoire plutôt qu'une fonction uniformément aléatoire, des contraintes plus souples pour obtenir des preuves face à des attaquants non-adaptatifs, etc.

7.2.1 Exemple

Nous allons reprendre le même exemple que pour les jeux. On souhaite majorer l'avantage de distinguer une permutation aléatoire d'une fonction aléatoire. Soit donc q et n des entiers positifs, avec $q \leq n$ et on définit Ω comme l'ensemble des $y = (y_1, \ldots, y_q) \in \mathcal{D}^q$ tels que les y_i sont deux à deux distincts. Ainsi, on remarque déjà que $|\Omega| \geq (1-\beta)|\mathcal{D}^q|$ avec $\beta = \frac{q(q-1)}{2\times 2^n}$ puisque, pour tout $i \neq j$, la probabilité que $y_i = y_j$ est égale à $\frac{1}{2^n}$ et il y a $\frac{q(q-1)}{2}$ choix pour (i,j). Calculons maintenant la probabilité que x soit envoyé sur y pour une fonction uniformément aléatoire puis pour une permutation uniformément aléatoire.

Pour une fonction uniformément aléatoire, puisque les entrées sont deux à deux distinctes, la probabilité que x soit envoyé sur y est exactement $\frac{1}{2^{nq}}$. Pour une permutation uniformément aléatoire, puisque les entrées et les sorties sont deux à deux distinctes, la probabilité x soit envoyé sur y est exactement $\prod_{i=0}^{q-1} \frac{1}{2^n - i}$. On remarque aisément que

$$\prod_{i=0}^{q-1} \frac{1}{2^n - i} \geq \frac{1}{2^{nq}} \ ,$$

et donc, le théorème des coefficients H, en utilisant $\alpha = 0$ et $\beta = \frac{q(q-1)}{2\times 2^n}$, permet de déduire que l'avantage pour distinguer une permutation uniformément aléatoire d'une fonction uniformément aléatoire est majoré par $\frac{q(q-1)}{2\times 2^n}$. La preuve est exclusivement calculatoire, plus rapide et assez intuitive.

7.2.2 Avantages

L'énoncé est « élémentaire » et ne nécessite aucune théorie préalable autre que les outils des probabilités élémentaires (contrairement au coupling ou aux systèmes aléatoires par exemple). Cela permet d'établir des preuves de sécurité assez facilement et rapidement nécessitant peu d'expérience dans ce domaine.

Cette technique translate le problème cryptographique en un problème combinatoire. Une fois la traduction en terme de comparaisons de probabilités effectuée, il s'agit « simplement » de calculs qui ne tiennent plus compte des attaquants, des oracles, du caractère adaptatif ou non, etc. Cela permet alors d'utiliser tous les outils habituels pour calculer des probabilités et utiliser les techniques combinatoires classiques.

Cette technique est optimale au sens où, en étudiant les probabilités d'envoyer les entrées sur les sorties, on trouvera soit une preuve de sécurité du schéma, soit une attaque. En effet, si certaines valeurs $\Pr[E(x) = y]$ sont faibles par rapport à $\Pr[f(x) = y]$, l'attaquant peut choisir ses requêtes de façon à construire avec une grande probabilité des uplets d'entrées/sorties x, y tels que $\Pr[E(x) = y]$ est éloignée de $\Pr[f(x) = y]$, permettant ainsi de distinguer les deux schémas. La façon d'utiliser les probabilités pour trouver une attaque est présentée en détail dans les articles [Pat91, Pat08]. Ainsi, il n'existe pas de preuve de sécurité utilisant une autre technique et qui ne pourrait être prouvée avec la technique des Coefficients H (contrairement au coupling par exemple).

Les coefficients H éliminent toutes les difficultés liées à l'adaptivité : il suffit de calculer des probabilités sans se soucier de l'adaptivité. C'est la principale difficulté des autres techniques.

Enfin, cette technique peut prouver des résultats du type « two weak make one strong », comme l'ont fait [CPS14].

7.2.3 Inconvénients

Les calculs peuvent s'avérer très difficiles et très complexes. D'autant plus que la complexité des calculs semble être croissante avec le nombre de tours du schéma (contrairement au coupling). Le calcul des probabilités d'envoyer les entrées sur les sorties prend en compte des objets qui ne rentrent pas intrinsèquement en jeu dans le calcul de l'indistinguabilité. Par exemple, pour le schéma d'Even-Mansour, l'indistinguabilité est intrinsèquement liée à la probabilité que des entrées (ou des sorties) collisionnent en entrée (ou en sortie) de la permutation interne P (ce que prennent en compte toutes les techniques), et la probabilité d'envoyer ces entrées sur ces sorties par P n'est pas importante mais elle rentre en compte dans les calculs avec la technique des coefficients H, ce qui contribue à la complexité des calculs.

7.3 Le coupling

Nous avons beaucoup étudié et détaillé cette technique dans les chapitres précédents et nous renvoyons le lecteur au chapitre 2 pour une présentation détaillée de la technique du coupling.

7.3.1 Exemple

En reprenant l'exemple précédemment utilisé, on est directement confronté à l'un des plus gros défaut du coupling : son incapacité à gérer l'adaptivité. Ainsi, si l'on cherche à distinguer une permutation uniformément aléatoire d'une fonction uniformément aléatoire, nous ne pouvons donner qu'un majorant ncpa, c'est-à-dire pour des requêtes directes non-adaptatives. Puisque nous avons très largement utilisé cette technique précédemment, sans introduire les notations et les étapes habituelles des preuves par coupling, nous présentons simplement l'idée générale. Il s'agit ici de considérer la distribution des $f(x_i)$, où f

est uniformément aléatoire, comme la distribution $\pi'(u_i)$ où π' est une permutation et les u_i sont uniformément aléatoires. Comme d'habitude, on a transporté l'aléa de la fonction sur l'aléa des entrées, maintenant ainsi la même distribution. Ainsi, on cherche à coupler la distribution des $\pi'(u_i)$ (distribution uniforme correspondant à la distribution pour une fonction uniformément aléatoire) et la distribution des $\pi(x_i)$ (la distribution d'une permutation uniformément aléatoire). Si u_i ne collisionne pas avec une entrée précédente, du type $u_i = x_j$ pour $j < i$, alors on peut coupler pour avoir $\pi'(u_i) = \pi(x_j)$. La probabilité de ne pas coupler la ℓ-ème requête est donc ici majorée par $\frac{\ell-1}{2^n}$ et l'avantage final est donc majoré par la somme sur les ℓ de 1 à q soit $\frac{q(q-1)}{2^{n+1}}$. On remarque ici que le résultat final est identique à celui obtenu par les jeux.

7.3.2 Avantages

Le principal avantage du coupling est sa capacité à utiliser et étendre une borne de sécurité sur un petit nombre de tours à une borne de sécurité sur un nombre arbitraire de tours. Typiquement, si l'on prouve avec la technique du coupling qu'un schéma E a une sécurité NCPA en $q \times \alpha$ où q est le nombre de requêtes et α un réel positif, alors il est très simple de prouver que le schéma E^r a une sécurité NCPA en $q \times \alpha^r$.

Par ailleurs, la valeur α est, en général, calculée assez simplement et correspond à la probabilité d'un certain événement intrinsèquement lié à l'indistinguabilité (en général la probabilité de certaines collisions).

7.3.3 Inconvénients

Le gros inconvénient du coupling est qu'il est très difficile de prouver des résultats optimaux pour des attaques CCA. En effet, jusqu'à maintenant, pour prouver une sécurité CCA, il a fallu doubler les tours pour utiliser un théorème du type « two weak make one strong » et ainsi, translater une borne NCPA en une borne CCA pour le double de tours. Théoriquement, il est possible de faire du coupling dans un cadre CCA mais, alors, pour tout $\ell \geq 1$, les probabilités de collisions pour la $\ell + 1$-ème requête sont des probabilités conditionnées par le fait que l'aléa est tel que les ℓ premières entrées sont envoyés sur les ℓ premières sorties. Modifiant ainsi l'uniformité de la distribution des clés et/ou des permutations/fonctions utilisées, rendant très difficiles les calculs.

Le coupling est également moins accessible que les coefficients H, par exemple, car cette technique nécessite d'introduire les notions de coupling en probabilité et une certaine méthodologie de preuve que nous avons présentée au chapitre 2.

7.4 Les systèmes aléatoires (Maurer)

La théorie des systèmes aléatoires a été créée en 2002 par Ueli Maurer [Mau02] et a permis de produire des résultats aussi bien pratiques que théoriques [MP04, Mau13, MPR07, MOPS06, MP03]. Cette théorie est la première à avoir prouvé le théorème « two weak make one strong » : la composition $E \circ F^{-1}$, avec E et F deux schémas de chiffrement par blos ncpa sûrs, est cca sûre. L'idée initiale de Maurer est d'unifier les différentes constructions cryptographiques et leur étude. Il remarque que la seule caractéristique importante d'un schéma pour étudier son indistinguabilité est la distribution des sorties étant donné un uplet d'entrée. Il choisit donc de créer des objets, appelés « systèmes aléatoires », uniquement caractérisés par une famille de distribution de probabilités.

7.4.1 Définitions

Système aléatoire

Plus concrètement, étant donné $\mathcal{X}$ et $\mathcal{Y}$ deux ensembles, un $(\mathcal{X}, \mathcal{Y})$-système aléatoire $\mathbf{F}$ prend des entrées $X_1, X_2, \ldots \in \mathcal{X}$ et, pour chaque entrée X_i, produit une sortie $Y_i \in \mathcal{Y}$ qui dépend des $X_1, \ldots, X_i$ et des $Y_1, \ldots, Y_{i-1}$. Ainsi, $\mathbf{F}$ peut être vu comme une suite de distributions de probabilités $P^F_{Y_i|X^iY^{i-1}}, i \geq 1$ où, pour tout $(x_1, \ldots, x_i, y_1, \ldots, y_i) \in \mathcal{X}^i \times \mathcal{Y}^i$, $P^F_{Y_i|X^iY^{i-1}}(y_i, x^i, y^{i-1})$ est la probabilité que $\mathbf{F}$ produise la sortie y_i sachant qu'il a reçu les i entrées $x_1, \ldots, x_i$ et produit les $i-1$ sorties $y_1, \ldots, y_{i-1}$. On remarque facilement qu'un schéma de chiffrement par blocs sur le domaine $\mathcal{D}$ est un $(\mathcal{D}, \mathcal{D})$-système aléatoire.

Distingueur

On peut, de manière similaire, modéliser un distingueur comme un système aléatoire. En effet, considérons un distingueur $\mathcal{D}$ déterministe qui interagit avec un $(\mathcal{X}, \mathcal{Y})$-système aléatoire $\mathbf{F}$. Le distingueur envoie toujours la même première requête X_1 à $\mathbf{F}$ et reçoit la réponse Y_i. A partir de cette réponse, il choisit X_2 en fonction de X_1, Y_1 et envoie la requête X_2. Il reçoit la réponse Y_2 et choisit X_3 en fonction des X_1, X_2, Y_1, Y_2. On remarque ainsi que $\mathcal{D}$ est déterminé par une famille de distribution de probabilités $P^{\mathcal{D}}_{X_i|X^{i-1}Y^{i-1}}, i \geq 1$ [1] ce qui est très proche de la définition d'un système aléatoire. Un distingueur n'est autre qu'un $(\mathcal{Y}, \mathcal{X})$-système aléatoire avec la donnée X_1 et produit un bit b après un certain nombre de requêtes q en fonction des valeurs $X_1, \ldots, X_q, Y_1, \ldots, Y_q$. On note E_q l'événement : $\mathcal{D}$ fixe b à 1 après q requêtes.

Avantage

Étant donné deux $(\mathcal{X}, \mathcal{Y})$-systèmes aléatoires $\mathbf{F}$ et $\mathbf{G}$ et un distingueur $\mathcal{D}$, on définit l'avantage de $\mathcal{D}$ comme la valeur $\left|P^{\mathcal{D}\mathbf{F}}(E_q) - P^{\mathcal{D}\mathbf{G}}(E_q)\right|$, où $P^{\mathcal{D}\mathbf{F}}(E_q)$ (respectivement $P^{\mathcal{D}\mathbf{G}}(E_q)$) est la probabilité que $\mathcal{D}$ fixe b à 1 après avoir interagi avec $\mathbf{F}$ (respectivement $\mathbf{G}$). Enfin, l'avantage maximal pour distinguer $\mathbf{F}$ de $\mathbf{G}$ est défini par

$$\Delta_q := \max_{\mathcal{D}} \left|P^{\mathcal{D}\mathbf{F}}(E_q) - P^{\mathcal{D}\mathbf{G}}(E_q)\right|,$$

où le max est pris sur tous les distingueurs faisant q requêtes.

Condition monotone

Une condition monotone est une suite d'événement $\mathcal{A} = A_1, A_2, \ldots$ telle que, si A_i est faux alors A_j reste faux pour tous les $j > i$. On peut, par exemple, penser à la suite d'événements $(A_i)_i$ définie par A_i est vrai si et seulement si les $Y_1, \ldots, Y_i$ sont deux à deux distincts. Dès lors qu'il y a une collision pour les indices j et k alors tous les indices $i \geq \max(j, k)$ vérifient A_i est faux.

Étant donné deux $(\mathcal{X}, \mathcal{Y})$-systèmes aléatoires $\mathbf{F}$ et $\mathbf{G}$ et une condition monotone $\mathcal{A} = A_1, A_2, \ldots$ dont les événements A_i dépendent des variables $X_1, \ldots, X_i, Y_1, \ldots, Y_i$ et potentiellement des variables internes de $\mathbf{F}$, on note $\mathbf{F}|A \equiv \mathbf{G}$ si, pour tout $i = 1..q$, on a $P^F_{Y_i|A_iX^iY^{i-1}} = P^G_{Y_i|X^iY^{i-1}}$. C'est-à-dire que, conditionné sur les événements A_i, les deux systèmes ont les mêmes distributions.

1. Un distingueur non-adaptatif vérifie $P^{\mathcal{D}}_{X_i|X^{i-1}Y^{i-1}} = P^{\mathcal{D}}_{X_i|X^{i-1}}, i \geq 1$

Un théorème fondamental des systèmes aléatoires établit que, pour de tels $\mathbf{F}$, $\mathbf{G}$ et $\mathcal{A}$, l'avantage pour distinguer $\mathbf{F}$ et $\mathbf{G}$ est majoré par la probabilité que A_q soit faux. Ce théorème est quasiment identique au théorème fondamental des jeux où l'on majore l'avantage par la probabilité qu'un événement se produise sachant que, quand cet événement est faux, les jeux sont similaires. On peut remarquer la similarité entre $\overline{A_q}$ et bad.

7.4.2 Exemple

Cherchons, comme précédemment, à distinguer une permutation uniformément aléatoire d'une fonction uniformément aléatoire. Soit $\mathbf{F}$ le système aléatoire qui correspond à une fonction uniformément aléatoire et $\mathbf{G}$ le système aléatoire qui correspond à une permutation uniformément aléatoire. On a, pour tout i :

$$P^F_{Y_i|X^iY^{i-1}} = \frac{1}{N} \text{ et } P^G_{Y_i|X^iY^{i-1}} = \frac{1}{N-i+1} \text{ si } Y_i \notin \{Y_1, \ldots, Y_{i-1}\},$$

où N est la taille des blocs.

Soit $\mathcal{A}$ la suite d'événements $(A_i)_i$ telle que A_i est vrai si $Y_1, \ldots, Y_i$ sont deux à deux distincts. Alors, le théorème fondamental des systèmes aléatoires dit que, puisque $\mathbf{F}|\mathcal{A} \equiv \mathbf{G}$, l'avantage pour distinguer $\mathbf{F}$ de $\mathbf{G}$ est majoré par la probabilité que A_q soit vrai, c'est-à-dire la probabilité qu'il y ait une collision parmi les variables uniformément aléatoires $Y_1, \ldots, Y_q$, c'est-à-dire une probabilité égale à $\frac{q(q-1)}{2^{n+1}}$.

7.4.3 Avantages

La théorie des systèmes aléatoires permet d'unifier l'étude des primitives et des constructions cryptographiques en considérant que la sécurité de ces objets est caractérisée par la famille des distributions des sorties conditionnées par les entrées et sorties précédentes. Ce point de vue permet d'établir des résultats généraux applicables largement. Par exemple, Maurer, Renner et Pietrzak [MPR07] ont prouvé des résultats d'amplification du type « two weak make one strong » en toute généralité pour des systèmes aléatoires. Cette théorie semble, à ce jour, la plus à même de prouver en toute généralité des théorèmes sur la sécurité des primitives et constructions cryptographiques. Dans la pratique, elle est proche de la technique par jeux et possède donc des avantages similaires. Ainsi, cette technique est applicable largement à des schémas de chiffrement par blocs mais également à d'autres constructions comme des MACs ou des fonctions de hachage. Elle est intuitive au sens où, comme pour les jeux, les calculs de la preuve se concentrent sur les événements intrinsèquement liés à l'indistinguabilité (comme les collisions).

7.4.4 Inconvénients

L'inconvénient majeur de cette technique est sa difficulté d'utilisation. Elle comporte des notations assez lourdes et un cadre de pensée inhabituel qui la rend difficile à manipuler au premier abord. Le paradoxe de cette technique est qu'elle est vouée à unifier les preuves de sécurité en apportant une abstraction et une rigueur mathématique mais, en pratique, c'est le contraire qui se produit : en 2012, Jetchev, Ozen et Stam [JÖS12] découvrent une erreur dans l'énoncé d'un lemme de Maurer [Mau02] dont la preuve, présentée par Pietrzak [Pie06], contient également une erreur. La lourdeur des notations rend difficile l'utilisation et la vérification des résultats prouvés par cette technique.

Bibliographie

[AGKS05] Masayuki Abe, Rosario Gennaro, Kaoru Kurosawa, and Victor Shoup. Tag-kem/dem: A new framework for hybrid encryption and a new analysis of kurosawa-desmedt kem. In *EUROCRYPT*, pages 128–146, 2005. 115

[AKKR08] Noga Alon, Tali Kaufman, Michael Krivelevich, and Dana Ron. Testing triangle-freeness in general graphs. *SIAM Journal on Discrete Mathematics*, 22(2):786–819, 2008. 77

[Bab89] Laszlo Babai. The fourier transform and equations over finite abelian groups: An introduction to the method of trigonometric sums. *Lecture notes, December 1989*, 1989. 77, 84, 85

[Ber05] Daniel J. Bernstein. A short proof of the unpredictability of cipher block chaining. Bernstein's website `cr.yp.to`, 2005. Available at `http://cr.yp.to/antiforgery/easycbc-20050109.pdf`. 118

[BKL+12] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, François-Xavier Standaert, John P. Steinberger, and Elmar Tischhauser. Key-Alternating Ciphers in a Provable Setting: Encryption Using a Small Number of Public Permutations - (Extended Abstract). In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 45–62. Springer, 2012. 21, 22, 23, 31, 118

[BKR98] Mihir Bellare, Ted Krovetz, and Phillip Rogaway. Luby-rackoff backwards: Increasing security by making block ciphers non-invertible. In *EUROCRYPT*, pages 266–280, 1998. 115

[BKR00] Mihir Bellare, Joe Kilian, and Phillip Rogaway. The Security of the Cipher Block Chaining Message Authentication Code. *Journal of Computer and System Sciences*, 61(3):362–399, 2000. 118

[BR93] Mihir Bellare and Phillip Rogaway. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. In *ACM Conference on Computer and Communications Security*, pages 62–73, 1993. 11

[BR00] John Black and Phillip Rogaway. Cbc macs for arbitrary-length messages: The three-key constructions. In *CRYPTO*, pages 197–215, 2000. 115

[BR02] John Black and Phillip Rogaway. A block-cipher mode of operation for parallelizable message authentication. In *EUROCRYPT*, pages 384–397, 2002. 115

[BR06] Mihir Bellare and Thomas Ristenpart. Multi-Property-Preserving Hash Domain Extension and the EMD Transform. In Xuejia Lai and Kefei Chen, editors, *Advances in Cryptology - ASIACRYPT 2006*, volume 4284 of *Lecture Notes in Computer Science*, pages 299–314. Springer, 2006. 117

[BRS02] John Black, Phillip Rogaway, and Thomas Shrimpton. Black-Box Analysis of the Block-Cipher-Based Hash-Function Constructions from PGV. In Moti Yung, editor, *Advances in Cryptology - CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 320–335. Springer, 2002. 115

[BRW04] Mihir Bellare, Phillip Rogaway, and David Wagner. The eax mode of operation. In *FSE*, pages 389–407, 2004. 115

[BW99] Alex Biryukov and David Wagner. Slide attacks. In *FSE*, pages 245–259, 1999. 75, 90

[BW00] Alex Biryukov and David Wagner. Advanced Slide Attacks. In Bart Preneel, editor, *Advances in Cryptology - EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 589–606. Springer, 2000. 23, 75, 90

[CLL+14] Shan Chen, Rodolphe Lampe, Jooyoung Lee, Yannick Seurin, and John P. Steinberger. Minimizing the two-round even-mansour cipher. In *Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I*, pages 39–56, 2014. 4, 24, 73

[CLP14] Benoit Cogliati, Rodolphe Lampe, and Jacques Patarin. The Indistinguishability of the XOR of k permutations. In *Fast Software Encryption - FSE 2014*, 2014. To appear. 4

[CPS14] Benoit Cogliati, Jacques Patarin, and Yannick Seurin. Security Amplification for the Composition of Block Ciphers: Simpler Proofs and New Results. In *Selected Areas in Cryptography - SAC 2014*, 2014. To appear. 18, 19, 48, 70, 120

[Cro00] Paul Crowley. Mercy: A Fast Large Block Cipher for Disk Sector Encryption. In Bruce Schneier, editor, *Fast Software Encryption - FSE 2000*, volume 1978 of *Lecture Notes in Computer Science*, pages 49–63. Springer, 2000. 38

[CS02] Ronald Cramer and Victor Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In *EUROCRYPT*, pages 45–64, 2002. 115

[CS03a] Jan Camenisch and Victor Shoup. Practical Verifiable Encryption and Decryption of Discrete Logarithms. In Dan Boneh, editor, *Advances in Cryptology - CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 126–144. Springer, 2003. 115

[CS03b] Ronald Cramer and Victor Shoup. Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack. *SIAM Journal on Computing*, 33(1):167–226, 2003. 115

[CS14] Shan Chen and John P. Steinberger. Tight security bounds for key-alternating ciphers. In *Advances in Cryptology - EUROCRYPT 2014*, Lecture Notes in Computer Science. Springer, 2014. 23, 40, 73, 80, 115

[Dae91] Joan Daemen. Limitations of the Even-Mansour Construction. In Hideki Imai, Ronald L. Rivest, and Tsutomu Matsumoto, editors, *Advances in Cryptology - ASIACRYPT '91*, volume 739 of *Lecture Notes in Computer Science*, pages 495–498. Springer, 1991. 23

[DDKS13] Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir. Key Recovery Attacks on 3-round Even-Mansour, 8-step LED-128, and Full AES^2. IACR Cryptology ePrint Archive, Report 2013/391, 2013. Available at `http://eprint.iacr.org/2013/391`. 24

[DKS12] Orr Dunkelman, Nathan Keller, and Adi Shamir. Minimalism in Cryptography: The Even-Mansour Scheme Revisited. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 336–354. Springer, 2012. 23, 24, 56, 73

[DR02] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer, 2002. 53

[DR07] Joan Daemen and Vincent Rijmen. Probability distributions of correlation and differentials in block ciphers. *J. Mathematical Cryptology*, 1(3):221–242, 2007. 55

[DS11] Yevgeniy Dodis and John P. Steinberger. Domain Extension for MACs Beyond the Birthday Barrier. In Kenneth G. Paterson, editor, *Advances in Cryptology - EUROCRYPT 2011*, volume 6632 of *Lecture Notes in Computer Science*, pages 323–342. Springer, 2011. 40

[EM97] Shimon Even and Yishay Mansour. A Construction of a Cipher from a Single Pseudorandom Permutation. *Journal of Cryptology*, 10(3):151–162, 1997. 21, 22, 33, 56

[FJM13] Pierre-Alain Fouque, Antoine Joux, and Chrysanthi Mavromati. Multi-user collisions: Applications to discrete logs, even-mansour and prince. *IACR Cryptology ePrint Archive*, 2013:761, 2013. 23

[FLS+10] Niels Ferguson, Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, and Jesse Walker. The Skein Hash Function Family. SHA3 Submission to NIST (Round 3), 2010. 38

[GGM99] S.W. Golomb, G. Gong, and L. Mittenthal. *Constructions of Orthomorphisms of Zn2*. Research report (University of Waterloo. Department of Combinatorics and Optimization). Faculty of Mathematics, University of Waterloo, 1999. 74

[GHL+07] David Goldenberg, Susan Hohenberger, Moses Liskov, Elizabeth Crump Schwartz, and Hakan Seyalioglu. On Tweaking Luby-Rackoff Blockciphers. In Kaoru Kurosawa, editor, *Advances in Cryptology - ASIACRYPT 2007*, volume 4833 of *Lecture Notes in Computer Science*, pages 342–356. Springer, 2007. 38

[GPPR11] Jian Guo, Thomas Peyrin, Axel Poschmann, and Matthew J. B. Robshaw. The LED Block Cipher. In Bart Preneel and Tsuyoshi Takagi, editors, *Cryptographic Hardware and Embedded Systems - CHES 2011*, volume 6917 of *Lecture Notes in Computer Science*, pages 326–341. Springer, 2011. 111

[GR04] Craig Gentry and Zulfikar Ramzan. Eliminating Random Permutation Oracles in the Even-Mansour Cipher. In Pil Joong Lee, editor, *Advances in Cryptology - ASIACRYPT 2004*, volume 3329 of *Lecture Notes in Computer Science*, pages 32–47. Springer, 2004. 24, 56

[Hay05] Thomas P. Hayes. A large-deviation inequality for vector-valued martingales. *2005*, 2005. 77

[HR03] Shai Halevi and Phillip Rogaway. A tweakable enciphering mode. In *CRYPTO*, pages 482–499, 2003. 115

[HR04] Shai Halevi and Phillip Rogaway. A parallelizable enciphering mode. In *CT-RSA*, pages 292–304, 2004. 115

[HR10] Viet Tung Hoang and Phillip Rogaway. On Generalized Feistel Networks. In Tal Rabin, editor, *Advances in Cryptology - CRYPTO 2010*, volume 6223 of *Lecture Notes in Computer Science*, pages 613–630. Springer, 2010. vii, 4, 20, 53, 54, 69, 70

[JÖS12] Dimitar Jetchev, Onur Özen, and Martijn Stam. Understanding adaptivity: Random systems revisited. In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology - ASIACRYPT 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 313–330. Springer, 2012. 118, 123

[JV04] Pascal Junod and Serge Vaudenay. Fox : A new family of block ciphers. In *Selected Areas in Cryptography*, pages 114–129, 2004. 74

[KPS13] Eike Kiltz, Krzysztof Pietrzak, and Mario Szegedy. Digital signatures with minimal overhead from indifferentiable random invertible functions. In Ran Canetti and JuanA. Garay, editors, *Advances in Cryptology - CRYPTO 2013*, volume 8042 of *Lecture Notes in Computer Science*, pages 571–588. Springer Berlin Heidelberg, 2013. 77, 84

[KR96] Joe Kilian and Phillip Rogaway. How to Protect DES Against Exhaustive Key Search. In Neal Koblitz, editor, *Advances in Cryptology - CRYPTO '96*, volume 1109 of *Lecture Notes in Computer Science*, pages 252–267. Springer, 1996. 3, 115

[KR01] Joe Kilian and Phillip Rogaway. How to Protect DES Against Exhaustive Key Search (an Analysis of DESX). *Journal of Cryptology*, 14(1):17–35, 2001. 21, 33

[Lin92] T. Lindvall. *Lectures on the Coupling Method*. Dover Books on Mathematics Series. Dover, 1992. 15

[LM90] Xuejia Lai and James L. Massey. A proposal for a new block encryption standard. In *EUROCRYPT*, pages 389–404, 1990. 74

[LP12] Rodolphe Lampe and Jacques Patarin. Analysis of some natural variants of the pkp algorithm. In *SECRYPT*, pages 209–214, 2012. 4

[LPS12] Rodolphe Lampe, Jacques Patarin, and Yannick Seurin. An Asymptotically Tight Security Analysis of the Iterated Even-Mansour Cipher. In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology - ASIACRYPT 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 278–295. Springer, 2012. 4, 19, 20, 22, 23

[LR86] Michael Luby and Charles Rackoff. Pseudo-random Permutation Generators and Cryptographic Composition. In *Symposium on Theory of Computing - STOC '86*, pages 356–363. ACM, 1986. 3

[LR88] Michael Luby and Charles Rackoff. How to Construct Pseudorandom Permutations from Pseudorandom Functions. *SIAM Journal on Computing*, 17(2):373–386, 1988. 53

[LRW02] Moses Liskov, Ronald L. Rivest, and David Wagner. Tweakable Block Ciphers. In Moti Yung, editor, *Advances in Cryptology - CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 31–46. Springer, 2002. 37, 38, 40

[LS13a] Rodolphe Lampe and Yannick Seurin. How to Construct an Ideal Cipher from a Small Set of Public Permutations. In *Advances in Cryptology - ASIACRYPT 2013*, 2013. To appear. Full version available at `http://eprint.iacr.org/2013/255`. 4

[LS13b] Rodolphe Lampe and Yannick Seurin. Tweakable Blockciphers with Asymptotically Optimal Security. In *Fast Software Encryption - FSE 2013*, 2013. To appear. 4, 19, 20, 39

[LS14] Rodolphe Lampe and Yannick Seurin. Security Analysis of Key-Alternating Feistel Ciphers. In *Fast Software Encryption - FSE 2014*, 2014. To appear. 4, 17, 19, 20, 53, 54

[LST12] Will Landecker, Thomas Shrimpton, and R. Seth Terashima. Tweakable Blockciphers with Beyond Birthday-Bound Security. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology - CRYPTO 2012*, volume 7417 of *Lecture Notes in Computer Science*, pages 14–30. Springer, 2012. 38, 39, 40, 118

[Mau92] Ueli M. Maurer. A Simplified and Generalized Treatment of Luby-Rackoff Pseudorandom Permutation Generator. In Rainer A. Rueppel, editor, *Advances in Cryptology - EUROCRYPT '92*, volume 658 of *Lecture Notes in Computer Science*, pages 239–255. Springer, 1992. 53

[Mau02] Ueli M. Maurer. Indistinguishability of Random Systems. In Lars R. Knudsen, editor, *Advances in Cryptology - EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 110–132. Springer, 2002. 3, 48, 115, 121, 123

[Mau13] Ueli Maurer. Conditional equivalence of random systems and indistinguishability proofs. In *Proceedings of the 2013 IEEE International Symposium on Information Theory, Istanbul, Turkey, July 7-12, 2013*, pages 3150–3154, 2013. 121

[Min09] Kazuhiko Minematsu. Beyond-Birthday-Bound Security Based on Tweakable Block Cipher. In Orr Dunkelman, editor, *Fast Software Encryption - FSE 2009*, volume 5665 of *Lecture Notes in Computer Science*, pages 308–326. Springer, 2009. 38

[Mir02] Ilya Mironov. (Not So) Random Shuffles of RC4. In Moti Yung, editor, *Advances in Cryptology - CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 304–319. Springer, 2002. 3, 134

[Mit95] L. Mittenthal. Block substitutions using orthomorphic mappings. *Advances in Applied Mathematics*, 16(1):59 – 71, 1995. 74

[MOPS06] Ueli M. Maurer, Yvonne Anne Oswald, Krzysztof Pietrzak, and Johan Sjödin. Luby-rackoff ciphers from weak round functions? In *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*, pages 391–408, 2006. 121

[MP03] Ueli M. Maurer and Krzysztof Pietrzak. The Security of Many-Round Luby-Rackoff Pseudo-Random Permutations. In Eli Biham, editor, *Advances in Cryptology - EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 544–561. Springer, 2003. 3, 53, 70, 115, 121

[MP04] Ueli M. Maurer and Krzysztof Pietrzak. Composition of Random Systems: When Two Weak Make One Strong. In Moni Naor, editor, *Theory of Cryptography Conference - TCC 2004*, volume 2951 of *Lecture Notes in Computer Science*, pages 410–427. Springer, 2004. 48, 115, 121

[MPR07] Ueli M. Maurer, Krzysztof Pietrzak, and Renato Renner. Indistinguishability Amplification. In Alfred Menezes, editor, *Advances in Cryptology - CRYPTO 2007*, volume 4622 of *Lecture Notes in Computer Science*, pages 130–149. Springer, 2007. 18, 19, 48, 70, 115, 121, 123

[MRS09] Ben Morris, Phillip Rogaway, and Till Stegers. How to Encipher Messages on a Small Domain. In Shai Halevi, editor, *Advances in Cryptology - CRYPTO 2009*, volume 5677 of *Lecture Notes in Computer Science*, pages 286–302. Springer, 2009. 3, 4, 19, 29, 45, 62

[Pat90] Jacques Patarin. Pseudorandom Permutations Based on the DES Scheme. In Gérard D. Cohen and Pascale Charpin, editors, *EUROCODE '90*, volume 514 of *Lecture Notes in Computer Science*, pages 193–204. Springer, 1990. 3, 53

[Pat91] Jacques Patarin. New Results on Pseudorandom Permutation Generators Based on the DES Scheme. In Joan Feigenbaum, editor, *Advances in Cryptology - CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 301–312. Springer, 1991. 3, 10, 23, 31, 48, 75, 81, 115, 118, 120

[Pat98] Jacques Patarin. About Feistel Schemes with Six (or More) Rounds. In Serge Vaudenay, editor, *Fast Software Encryption - FSE '98*, volume 1372 of *Lecture Notes in Computer Science*, pages 103–121. Springer, 1998. 3

[Pat03] Jacques Patarin. Luby-Rackoff: 7 Rounds Are Enough for $2^{n(1-\epsilon)}$ Security. In Dan Boneh, editor, *Advances in Cryptology - CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 513–529. Springer, 2003. 3

[Pat04] Jacques Patarin. Security of Random Feistel Schemes with 5 or More Rounds. In Matthew K. Franklin, editor, *Advances in Cryptology - CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 106–122. Springer, 2004. 3, 53

[Pat08] Jacques Patarin. The "coefficients h" technique. In *Selected Areas in Cryptography*, pages 328–345, 2008. 10, 23, 31, 48, 75, 81, 115, 118, 120

[Pat10] Jacques Patarin. Security of balanced and unbalanced Feistel Schemes with Linear Non Equalities. *IACR Cryptology ePrint Archive, Report 2010/293*, 2010. Available at `http://eprint.iacr.org/2010/293`. 53

[Pie06] Krzysztof Pietrzak. *Indistinguishability and composition of random systems*. PhD thesis, ETH Zurich, 2006. 123

[RBBK01] Phillip Rogaway, Mihir Bellare, John Black, and Ted Krovetz. Ocb: a block-cipher mode of operation for efficient authenticated encryption. In *ACM Conference on Computer and Communications Security*, pages 196–205, 2001. 115

[Rog02] Phillip Rogaway. Authenticated-encryption with associated-data. In *ACM Conference on Computer and Communications Security*, pages 98–107, 2002. 115

[Rog04] Phillip Rogaway. Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. In Pil Joong Lee, editor, *Advances in Cryptology - ASIACRYPT 2004*, volume 3329 of *Lecture Notes in Computer Science*, pages 16–31. Springer, 2004. 38, 115

[RR00] Zulfikar Ramzan and Leonid Reyzin. On the Round Security of Symmetric-Key Cryptographic Primitives. In Mihir Bellare, editor, *Advances in Cryptology - CRYPTO 2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 376–393. Springer, 2000. 56

[Sch98] Richard Schroeppel. The Hasty Pudding Cipher. AES submission to NIST, 1998. 38

[Sho96] Victor Shoup. On Fast and Provably Secure Message Authentication Based on Universal Hashing. In Neal Koblitz, editor, *Advances in Cryptology - CRYPTO '96*, volume 1109 of *Lecture Notes in Computer Science*, pages 313–328. Springer, 1996. 42

[Sho00] Victor Shoup. Using hash functions as a hedge against chosen ciphertext attack. In *EUROCRYPT*, pages 275–288, 2000. 115

[Sho01] Victor Shoup. Oaep reconsidered. In *CRYPTO*, pages 239–259, 2001. 115

[SS00] Thomas Schweinberger and Victor Shoup. Ace: The advanced cryptographic engine. *IACR Cryptology ePrint Archive*, 2000:22, 2000. 115

[Ste12] John Steinberger. Improved Security Bounds for Key-Alternating Ciphers via Hellinger Distance. IACR Cryptology ePrint Archive, Report 2012/481, 2012. Available at `http://eprint.iacr.org/2012/481`. 22, 23, 118

[Ste13] John Steinberger. Counting solutions to additive equations in random sets. arXiv Report 1309.5582, 2013. Available at `http://arxiv.org/abs/1309.5582`. 77, 84, 85, 86

[Vau98] Serge Vaudenay. Provable security for block ciphers by decorrelation. In *STACS*, pages 249–275, 1998. 3

[Vau99] Serge Vaudenay. On the lai-massey scheme. In *ASIACRYPT*, pages 8–19, 1999. 74

[Vau03] Serge Vaudenay. Decorrelation: A Theory for Block Cipher Security. *Journal of Cryptology*, 16(4):249–286, 2003. 53

[Yas10] Kan Yasuda. The Sum of CBC MACs Is a Secure PRF. In Josef Pieprzyk, editor, *Topics in Cryptology - CT-RSA 2010*, volume 5985 of *Lecture Notes in Computer Science*, pages 366–381. Springer, 2010. 40

[Yas11] Kan Yasuda. A New Variant of PMAC: Beyond the Birthday Bound. In Phillip Rogaway, editor, *Advances in Cryptology - CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 596–609. Springer, 2011. 40

Résumé

Dans cette thèse, on s'intéresse à des schémas de chiffrement par blocs, c'est-à-dire que le chiffrement (et le déchiffrement) envoie un bloc de n bits sur un bloc de n bits. Il y a essentiellement deux grandes structures utilisées pour un schéma de chiffrement par blocs : la structure de Feistel (utilisée pour le DES) et la structure SPN (utilisée pour l'AES). L'étude de la sécurité de ces différents structures et schémas a permis de nombreuses avancées autant pratiques que théoriques. Nous présentons dans cette thèse des preuves de sécurité pour le schéma d'Even-Mansour itéré, le schéma paramétrable CLRW et le schéma de Feistel à clés alternées. Ces preuves utilisent une technique probabiliste, appelée coupling, introduite en cryptographie en 2002 par Mironov [Mir02]. Nous présentons cette technique dans le cadre des probabilités, puis la façon d'utiliser le coupling pour prouver la sécurité des schémas cités précédemment. Nous présentons également une étude de la sécurité du schéma d'Even-Mansour à deux tours pour certaines minimisations (même clés de tours ou même permutations internes par exemple) et, pour conclure, une comparaison des différentes techniques d'indistinguabilité.

Abstract

In this thesis, we study blockciphers, meaning that the encryption (and decryption) sends a block of n bits on a block of n bits. There is essentially two main structures used for a blockcipher: the Feistel structure (used for DES) and the SPN structure (used for AES). The study of the security of these structures and schemes has led to many practical and theoretical advances. We present in this thesis proofs of security for the iterated Even-Mansour scheme, the tweakable blockcipher CLRW and the key-alternating Feistel cipher. These proofs use a probabilistic technique, called coupling, introduced in cryptography in 2002 by Mironov [Mir02]. We present this technique in the context of probabilities, then we present how to use the coupling to prove the security for the schemes mentioned above. We also present an analysis of the security of the Even-Mansour cipher with two rounds and some properties (same round keys or same internal permutations for example) and, finally, we compare the different techniques to prove indistinguishability.