Transducteurs finis dans la clé publique Cryptographie

Joana Barão Vieira

Master en sécurité de l'information

Département des sciences informatiques

2017

Orientateur

Rogério Ventura Lages dos Santos Reis, professeur auxiliaire,
Faculté des Sciences de l'Université de Porto

Coordinateur

Ivone de Fátima da Cruz Amorim, ,
Centre de mathématiques de l'Université de Porto

FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

Toutes les corrections déterminées

pelo júri, et só essas, foram efetuadas.

Monsieur le Président de la Cour,

Porto, ______/______/________

MSC

Dédié à mes parents, pour tout l'argent dépensé pour mon éducation

Abstrait

La cryptographie est utilisée pour sécuriser les communications depuis des milliers d'années. Cependant, aujourd'hui, La cryptographie est confrontée à de nouveaux défis. L'augmentation de la puissance de calcul, l'utilisation croissante de petits des appareils tels que les cartes à puce, ainsi que la possibilité que l'informatique quantique devienne une réalité, nécessitent de nouveaux systèmes cryptographiques qui offrent une sécurité reposant sur des hypothèses différentes des systèmes classiques De plus, il est nécessaire d'utiliser des clés de petite taille ainsi qu'un cryptage et un décryptage rapides.

Les cryptosystèmes à clé publique à automates finis, FAPKC, sont des systèmes basés sur des transducteurs finis, qui répondent aux exigences précédentes. Leur sécurité ne repose pas sur des hypothèses de complexité liés aux problèmes de théorie des nombres, comme les problèmes classiques. De plus, ces cryptosystèmes offrent des des clés de petite taille ainsi qu'une complexité des temps de chiffrement et de déchiffrement linéaires.

Comme dans d'autres cryptosystèmes, un concept fondamental de FAPKC est la capacité d'inverser le procédure de cryptage, d'une manière qui est difficile à quiconque, sauf au propriétaire de la clé privée. Dans ce sens, ces cryptosystèmes dépendent fortement des résultats d'inversibilité des transducteurs finis, comme ainsi que les résultats sur le produit spécial utilisé pour générer la clé publique. Dans cette thèse, nous étudions ces deux concepts et présentons une grande variété d'exemples afin d'aider les lecteurs pour les comprendre.

Les principales contributions de ce travail sont la définition étendue des transducteurs finis quasi-linéaires avec mémoire, la formalisation d'une procédure pour vérifier l'injectivité et construire des inverses de finis transducteurs à mémoire (linéaire et quasi-linéaire) et l'extension à l'attaque Bao-Igarashi à FAPKC à toutes les valeurs possibles du délai d'injectivité.

Mots clés : transducteurs finis, inversibilité, composition, attaque FAPKC.

Résumé

La cryptographie vous permet d'être utilisée pour communiquer en toute sécurité pendant des millions d'années. Non, aujourd'hui, la cryptographie s'applique à de nouveaux défis. L'augmentation de la puissance informatique, l'utilisation du croissant de petits appareils comme les cartes à puce, ainsi que la possibilité d'un ordinateur quantique se tornar realidade, requerem de novos sistemas cryptogr´aficos qui ofere¸cam seguran¸ca baseada em pressupostos diferentes dos cl´assicos. Al'em disso, 'e necess'ario pequenos tamanhos de chave, bem como processos de cifrar e decifrar r´apidos.

Les automates finis, les cryptosystèmes à clé publique, les FAPKC et les systèmes basés sur les transducteurs finitos, que preenchem os requisitos anteriores. La sécurité de ces systèmes ne dépend pas de pressions de complexité liées aux problèmes de théorie des nombres, comme classiques. D'autre part, les systèmes FAPKC offrent des tamanhos de chave relativement petits, asim como tempo linear a cifrar e decifrar.

Comme d'autres systèmes cryptographiques, un concept fondamental de nos FAPKC, leur capacité de l'onduleur à cifra, de forme qui est difficile pour tout personnel exceto pour le propriétaire du chave privada. Neste sentido, ces systèmes dépendent fortement des résultats liés avec l'invertibilité des transducteurs finis et, pour eux, les résultats liés à o produit spécial utilisé pour gerar a chave publica. Nesta disserta¸c˜ao, estudamos estes conceitos Nous présentons une grande variété d'exemples pour aider les lecteurs à les comprendre.

As principais contribui¸c˜oes deste trabalho s˜ao a defini¸c˜ao estendida de transdutores finitos quase linéaires avec mémoire, formalisation d'une procédure pour vérifier l'imagination et la construction inverses de transducteurs finis avec mémoire (linéaires et quasi-linéaires) et extensions du Bao-Igarashi s'attaque au FAPKC pour toutes les valeurs possibles pour l'attraction de l'imagination.

Contenu

Liste des tableaux

Liste des figures

Chapitre 1

Introduction

La cryptographie est utilisée pour sécuriser les communications depuis des milliers d'années. L'histoire montre que la communication militaire a eu la plus grande influence sur la cryptographie et ses ad- Les progrès technologiques. Le besoin de communications commerciales et privées sécurisées a été stimulé par la L'ère de l'information. Jusqu'à l'invention de la cryptographie à clé publique, tous les chiffrements étaient symétriques. La cryptographie symétrique utilise des algorithmes dotés d'une clé pour crypter et décrypter les informations. Cela signifie que chaque partie à la communication a besoin de la même clé, celle de l'expéditeur pour crypter le message et le destinataire pour le décrypter. Cela posait un problème important : avant pouvait communiquer en toute sécurité, il était nécessaire d'échanger un secret avec le partenaire. Clé publique Les cryptosystèmes ont révolutionné la cryptographie en simplifiant considérablement cette distribution de clés processus. Plutôt que de partager des clés secrètes, les utilisateurs peuvent désormais transmettre leur clé publique à d'autres parties. Cette clé publique permettait à l'expéditeur de crypter, mais elle ne pouvait pas être utilisée pour effectuer l'opération. opération de décryptage correspondante. Cette partie serait effectuée avec le privé correspondant clé, gardée secrète par le destinataire.

Le concept de cryptographie à clé publique a été introduit par Diffie, Hellman et Merkle en 1976. En 1978, Rivest, Shamir et Adleman ont présenté le premier cryptosystème à clé publique, appelé RSA [Dif88]. Sa sécurité est liée à la difficulté de factoriser de grands entiers. Le ElGamal Le cryptosystème, inventé par Taher ElGamal en 1985 [ElG85], repose sur un problème similaire, le problème du logarithme discret. Toujours en 1985, Neal Koblitz [Kob87] et Victor Miller [Mil85], indépendamment, a introduit la cryptographie à courbe elliptique, basée sur la courbe elliptique discrète problème de logarithme. Bien que mathématiquement plus complexes, les courbes elliptiques fournissent des clés plus petites tailles et des opérations plus rapides pour une sécurité estimée à peu près équivalente. Depuis les années 1970, un une grande variété de cryptosystèmes à clé publique ont été développés, la plupart d'entre eux basés sur la complexité hypothèses liées aux mêmes problèmes de théorie des nombres que RSA et ElGamal. Cette dépendance sur un très petit ensemble de problèmes, ces cryptosystèmes deviennent quelque peu vulnérables.

Dans une série d'articles [TCC97, TC97, TC99], Renji Tao a introduit une famille de cryptosystèmes basé sur des transducteurs finis, appelés FAPKC (qui signifie Finite Automata Public Key) Cryptosystèmes). La sécurité de ces cryptosystèmes ne repose pas sur des hypothèses de complexité liés aux problèmes de théorie des nombres, s'appuyant plutôt sur la difficulté d'inverser les nombres finis non linéaires transducteurs et de factorisation de polynômes matriciels sur Fq [Tao09], tous deux des problèmes NP. cette famille de cryptosystèmes utilise des tailles de clé relativement petites, un cryptage et un décryptage rapides et peut également être utilisé pour la signature. L'implémentation de FAPKC ne nécessite que des opérations logiques, le rendant adapté aux applications de cartes à puce [TC97].

Dans les FAPKC, grosso modo, la clé privée se compose de deux transducteurs finis avec mémoire, une linéaire et une quasi-linéaire. La clé publique est obtenue par un produit spécial de l'original paire, ce qui donne un transducteur fini non linéaire avec mémoire. On ne connaît pas d'algorithme pour inverser les transducteurs finis non linéaires, ni les factoriser. Par conséquent, pour inverser la transducteur à clé publique, il faut les inverses de ses facteurs, qui sont facilement calculés à partir de la transducteurs dans la clé privée. La principale différence entre les différentes variantes de FAPKC est le choix du type de transducteurs pour la clé privée.

Bien que certains schémas FAPKC se soient déjà avérés non sécurisés [BI95], ces cryptosystèmes continuent de se présenter comme une bonne alternative aux classiques. Malgré les nombreux avantages de FAPKC, son étude a été en quelque sorte condamnée par le fait que de nombreux articles ont été rédigés en un langage aride, avec de nombreux résultats présentés sans preuve ni exemples, et d'autres se référant Documents chinois. Quelques éclaircissements et consolidations des travaux déjà réalisés sur ce sujet ont été présentés par Ivone Amorim, Ant´onio Machiavelo et Rog´erio Reis dans une série de communications [AMR12, AMR14a, AMR14b, AMR14c] et une thèse de doctorat [dCA16]. Dans ces travaux, il a été présenté de manière plus claire certains résultats déjà connus, on a étudié le nombre et la taille des classes d'équivalence de transducteurs finis linéaires définis sur Fq, ainsi que des algorithmes pour vérifier inversibilité et inversement des transducteurs linéaires à mémoire. Cette thèse est la continuation de ce travail.

Dans ce travail, après avoir présenté quelques résultats connus sur les transducteurs finis linéaires et les transducteurs finis, transducteurs à mémoire, nous introduisons une nouvelle définition « étendue » des transducteurs finis quasi-linéaires avec mémoire, permettant l'augmentation des clés privées possibles. Ensuite, nous introduisons et formalisons un procédure de vérification de l'injectivité des transducteurs finis linéaires et quasi-linéaires, ainsi qu'une et condition suffisante pour l'injectivité de ces transducteurs. Inversion linéaire et quasi-linéaire Les transducteurs à mémoire sont fondamentaux dans le processus de génération de clés des FAPKC, car un doit définir à la fois un transducteur inversible avec mémoire et un inverse correspondant. afin de pouvoir étudier les FAPKC préexistantes, nous présentons deux types de compositions de transducteurs à mémoire, introduits par Tao [Tao09]. De plus, un schéma général sera illustré de génération de clés et de processus de chiffrement et de déchiffrement. Le schéma présenté est connu pour être incertain, cependant, c'est le seul que nous pouvons comprendre à travers les documents auxquels nous avons eu accès. Enfin, nous présenterons l'attaque Bao-Igarashi à ce schéma et l'étendrons pour qu'elle fonctionne avec tous les valeurs possibles du retard d'injectivité des transducteurs. Tout au long de ce travail, il est présent une grande variété d'exemples pour illustrer les concepts et procédures introduits.

1.1 Structure de cette thèse

Nous commençons par passer en revue, au chapitre 2, plusieurs concepts et résultats issus de différents domaines des mathématiques. matiques qui seront utilisées tout au long de ce travail. Nous introduisons également quelques notations pratiques.

Les notions préliminaires et les résultats des transducteurs finis généraux sont donnés au chapitre 3, y compris les notions d'injectivité et d'inversibilité qui sont considérées dans ce travail. De plus, dans ce chapitre, nous donnons les définitions de transducteur fini linéaire et de transducteur fini à mémoire (linéaire et quasi-linéaire). Ensuite, nous présentons notre nouvelle définition étendue des transducteurs finis quasi-linéaires avec mémoire. Certains résultats sur l'inversibilité des transducteurs finis avec mémoire sont également présentés dans ce chapitre.

Au chapitre 4, une condition nécessaire et suffisante à l'inversibilité des fonctions finies linéaires est donnée. transducteurs à mémoire. Nous présentons et formalisons une procédure pour vérifier l'injectivité des transducteurs linéaires transducteurs finis à mémoire, utilisant les transformations R_a et R_b . Au cours de cette procédure, nous construire un transducteur inverse de l'original. De plus, ces résultats sont étendus aux transducteurs quasi-linéaires transducteurs finis avec mémoire.

Le chapitre 5 est consacré à la présentation de l'attaque Bao-Igarashi à FAPKC. Afin de pouvoir Pour ce faire, nous commençons par introduire deux compositions différentes de transducteurs finis. Ensuite, nous présentons une description générale de FAPKC ainsi qu'un schéma de base avec génération de clés et cryptage et les processus de décryptage. Enfin, il est présenté l'attaque Bao-Igarashi modifiée pour fonctionner avec toutes les valeurs possibles du délai d'injectivité et l'illustrer à travers un exemple.

Pour terminer, dans le chapitre 6, nous résumons nos contributions et discutons de certaines orientations de recherche futures.

Chapitre 2

Prérequis mathématiques

2.1 Relations et fonctions

Soient A et B deux ensembles. Une relation de A vers B est un sous-ensemble du produit cartésien A × B.

La notation a b est utilisée pour indiquer que (a, b) est dans la relation . Si (a, b) n'est pas dans la relation , on le note a b. Lorsque A = B, est également appelé une relation binaire sur A.

Une relation binaire sur un ensemble A est dite une relation d'équivalence si et seulement si les conditions suivantes les conditions sont réunies :

- est réflexif, c'est-à-dire a a, pour tout a dans A ;
- est symétrique, c'est-à-dire a b si et seulement si b a, pour tout a, b dans A ;
- est transitif, c'est-à-dire que si a b et b c, alors a c, pour tout a, b, c dans A.

Soit une relation d'équivalence sur A. Pour tout a A, l'ensemble [a] = {b A | a b} est appelé la classe d'équivalence contenant a, tandis que l'ensemble de toutes les classes d'équivalence, A/ = {[a] | a A}, est appelé le quotient de A par .

La restriction d'une relation binaire sur un ensemble A à un sous-ensemble S est l'ensemble de toutes les paires (a, b) dans le relation pour laquelle a et b sont dans S. Si une relation est une relation d'équivalence, ses restrictions sont aussi.

Étant donné un entier positif n, un exemple de relation d'équivalence est la congruence modulo n relation sur l'ensemble des entiers, Z. Pour un entier positif n, on définit cette relation sur Z comme suit. Deux entiers a et b sont dits congruents modulo n, écrits :

$$a \equiv_n b \text{ ou } a \equiv b \pmod{n},$$

si leur différence a − b est un multiple de n. Il est facile de vérifier qu'il s'agit d'une relation d'équivalence sur les entiers. Le nombre n est appelé le module. Une classe d'équivalence se compose de ceux entiers qui ont le même reste lors de la division par n. L'ensemble des entiers modulo n, qui est noté Zn, est l'ensemble de toutes les classes de congruence des entiers pour le module n.

Exemple 2.1.1. Prenons n = 2. Ensuite, par exemple,

$$5 \equiv 3 \equiv 1 \pmod{2} \text{ et } [1] \quad = \{2j + 1 \mid j \quad Z\}.$$

Une relation d'un ensemble A à un ensemble B est appelée fonction, carte ou application, si chaque élément de A est se rapportant exactement à un élément de B. Une fonction f de A vers B est notée f : A → B, et pour tout a dans A, f(a) désigne l'élément dans B qui est lié à a, qui est généralement appelé l'élément image d'un sous f.

Une fonction f : A → B est dite injective, ou fonction bijective, si elle satisfait les conditions suivantes condition:

$$a, a \quad A, f(a) = f(a\ ) \quad a = a \qquad ,$$

et est dit surjectif si la condition suivante est remplie :

$$b \quad B, \quad a \quad A, f(a) = b.$$

Si une fonction est à la fois injective et surjective, alors elle est appelée bijective ou bijection.

2.2 Groupes, anneaux et corps

Soit A un ensemble et n un nombre naturel. Une opération n-aire sur A est une application de An vers A. L'opération : A2 → A est appelée une opération binaire, ce qui signifie seulement que si (a, b) est un paire ordonnée d'éléments de A, alors ab est un élément unique de A.

Un groupe est une paire ordonnée (G,), où G est un ensemble non vide et est une opération binaire sur G (appelée opération de groupe), satisfaisant les propriétés suivantes :

- l'opération est associative, c'est-à-dire $x(yz) = (xy)z$, pour tout $x, y, z \in G$;
- il existe un élément $e \in G$ tel que $xe = ex = x$, pour tout x dans G. Un tel élément est unique et est appelé élément d'identité ;
- si x est dans G, alors il existe un élément y dans G tel que $xy = yx = e$, où e est le élément d'identité. Cet élément y est appelé l'inverse de x.

Un groupe est noté de manière additive (multiplicative) ou est un groupe additif (multiplicatif) lorsque :

- l'opération de groupe est notée $+$ $(\cdot)$;
- l'élément d'identité est noté 0 (1) ;
- l'inverse d'un élément x est noté $-x$ (x^{-1}),

respectivement. Si l'opération de groupe est commutative, c'est-à-dire $xy = yx$ pour tout x, y dans G, alors G est appelé groupe abélien ou groupe commutatif.

Il existe quelques exemples très familiers de groupes abéliens sous addition, à savoir les entiers $\mathbb{Z}$, les rationnels $\mathbb{Q}$, les nombres réels $\mathbb{R}$ et $\mathbb{Z}_n$, pour $n \in \mathbb{N}$. Notez que $\mathbb{N}$ désigne l'ensemble des nombres naturels nombres, c'est-à-dire $\mathbb{N} = \{1, 2, 3, \ldots\}$.

Un anneau est un triplet ordonné $(R, +, \cdot)$, où R est un ensemble non vide, $+$ est une opération binaire sur R est appelée addition, et $\cdot$ est également une opération binaire sur R appelée multiplication, qui obéit à la règles suivantes:

- $(R, +)$ est un groupe abélien (l'identité additive est notée 0) ;
- l'opération multiplicative est associative, c'est-à-dire $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, pour tout x, y, z dans R ;
- il existe un élément 1 dans R tel que $1 \cdot x = x \cdot 1 = x$, pour tout x dans R. 1 est appelé le identité multiplicative ;
- la multiplication est distributive à gauche par rapport à l'addition, c'est-à-dire $x \cdot (y+z) = x \cdot y + x \cdot z$, pour tous x, y, z dans R ;
- la multiplication est distributive à droite par rapport à l'addition, c'est-à-dire $(x+y) \cdot z = x \cdot z + y \cdot z$, pour tous x, y, z dans R.

Un exemple simple d'anneau est l'ensemble des entiers avec les opérations habituelles d'addition et multiplication.

Soit R un anneau d'identité multiplicative 1. Un élément r dans R est dit multiplicativement inversible ou simplement inversible si et seulement s'il existe un élément s dans R tel que $r \cdot s = s \cdot r = 1$, et s est appelé l'inverse multiplicatif de r ou simplement l'inverse de r. Un élément inversible dans R est appelé une unité et l'ensemble des unités de R est représenté par R . Soit a, b R. On dit que a divise b, et on écrit $a \mid b$, s'il existe q R tel que $b = aq$, où aq abrège $a \cdot q$.
La définition de la relation de congruence modulo n sur l'ensemble des entiers, présentée précédemment, peut être généralisée aux éléments d'un anneau. Ainsi, deux éléments a, b dans un anneau, R, sont congruents modulo n R si $n \mid (a - b)$.

Un corps est un anneau commutatif qui possède des inverses multiplicatifs pour tous les éléments non nuls. des nombres réels, ainsi que les opérations habituelles d'addition et de multiplication, constituent un corps.

Si F est un corps avec un nombre fini d'éléments, alors on dit que F est un corps fini ou un corps de Galois. Les exemples les plus simples de corps finis sont les corps premiers : étant donné un nombre premier p, le corps premier Le corps F_p ou GF(p) est l'ensemble des entiers modulo p, précédemment noté Z_p. Les éléments d'un corps premier peuvent être représentés par des entiers compris entre 0, 1, . . . , p−1. Par exemple, $F_2 = \{0, 1\}$.

2.3 Modules et espaces vectoriels

Soit R un anneau et 1 son identité multiplicative. Un R-module à droite, M, est constitué d'un abélien groupe (M, +) et une opération : $M \times R \to M$ telle que, pour tout r, s R et x, y M :

- (x + y) r = x r + y r
- x (r + s) = x r + x s
- x (rs) = (x r) s
- x 1 = x.

L'opération de l'anneau sur M est appelée multiplication scalaire et s'écrit généralement par juxtaposition, c'est-à-dire xr pour r R et x M. Cependant, dans la définition ci-dessus, elle est notée x r pour le distinguer de l'opération de multiplication en anneau, qui est notée par juxtaposition. Une gauche Le R-module M est défini de manière similaire, sauf que l'anneau agit à gauche, c'est-à-dire la multiplication scalaire prend la forme : R × M → M et les axiomes ci-dessus s'écrivent avec des scalaires r et s sur le à gauche de x et y.

Si R est commutatif, alors les R-modules de gauche sont les mêmes que les R-modules de droite et sont simplement appelés Modules R.

Par exemple, si R est un anneau commutatif et n N, alors R^n est à la fois un R-module gauche et un R-module droit. si l'on utilise les opérations composant par composant :

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n),$$

$$\alpha(a_1, a_2, \ldots, a_n) = (\alpha a_1, \alpha a_2, \ldots, \alpha a_n),$$

pour tout $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n)$ R^n, et pour tout α R.

Soit F un corps. Alors un F-module est appelé un espace vectoriel sur F.

Exemple 2.3.1. Soit n N. L'ensemble F_2^n avec les opérations composante par composante d'addition et la multiplication scalaire, telle que définie ci-dessus, est un espace vectoriel sur le corps F_2 qui est noté simplement par F_2^n.

Soit V un espace vectoriel sur un corps F. Un sous-ensemble non vide U de V est dit sous-espace de V si U est lui-même un espace vectoriel sur F avec les mêmes opérations que V .

Soit V un espace vectoriel sur un corps arbitraire F et n N. Un vecteur de la forme

$$\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n,$$

où α_i F et v_i V , pour i = 1, . . . , n, est appelée une combinaison linéaire des vecteurs $v_1, v_2, \ldots,$ v_n. Le scalaire α_i est appelé le coefficient de v_i , pour i = 1, . . . , n.

L'ensemble de toutes les combinaisons linéaires de vecteurs donnés $v_1, v_2, \ldots, v_n$ V est un sous-espace de V et est appelé le sous-espace engendré par (ou engendré par) les vecteurs $v_1, v_2, \ldots,$ v_n.

Soit $S = \{s_1, s_2, \ldots, s_n\}$ un sous-ensemble non vide de V et v V . S'il existe des scalaires $\alpha_1, \alpha_2, \ldots,$ un dans F tel que

$$v = \alpha_1 s_1 + \alpha_2 s_2 + \ldots + a_m s_n,$$

alors on dit que v peut s'écrire comme une combinaison linéaire des vecteurs dans S. L'ensemble S est linéairement indépendant si et seulement si aucun vecteur dans S ne peut être écrit comme une combinaison linéaire des autres vecteurs de cet ensemble. Si un vecteur de S peut être écrit comme une combinaison linéaire des autres, alors l'ensemble des vecteurs est dit linéairement dépendant.

Un sous-ensemble non vide B de V est dit base de V si et seulement si les deux conditions suivantes sont remplies vrai:

- B est un ensemble linéairement indépendant ;
- V est enjambé par B.

Exemple 2.3.2. Il est facile de voir que l'ensemble {(1, 0, 0); (0, 1, 0); (0, 0, 1)} est une base de R^3, lequel est appelée la base standard de R^3.

Si V est un espace vectoriel qui a une base B contenant un nombre fini de vecteurs, alors V est dit être de dimension finie. Le nombre d'éléments sur cette base est ce qu'on appelle la dimension de V , et est noté dim(V). On peut montrer que la dimension d'un espace vectoriel ne dépendent de la base choisie, puisque toutes les bases ont le même nombre d'éléments [Val93]. Si V n'a pas de base finie, alors V est dit de dimension infinie.

Exemple 2.3.3. D'après l'exemple précédent, il est clair que R^3 est de dimension finie et son la dimension est 3.

2.4 Matrices et forme normale de Smith

Soit m, n N et R un corps. Soit $a_{i,j}$ R, pour i = 1, . . . , m et j = 1, . . . ,n. Le corps rectangulaire tableau A défini par

$$A = [a_{i,j}] = \begin{matrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \text{suis}_{,1} & \text{suis}_{,2} & \cdots & \text{suis}_{,n} \end{matrix}$$

est appelée une matrice sur R avec m lignes et n colonnes, ou simplement une matrice m × n. Si m = n on dit que A est une matrice carrée. Si m = n, alors la matrice est dite non carrée. L'ensemble de tous les matrices sur R avec m lignes et n colonnes sont notées $M_{m\times n}(R)$. Si m = n, on note $M_{n\times n}(R)$ simplement par $M_n(R)$. Les éléments d'une matrice sont appelés ses entrées, et $a_{i,j}$ désigne l'entrée qui apparaît à l'intersection de la ième ligne et de la jième colonne.

Une matrice dans $M_{m\times n}(R)$ ($M_n(R)$) dans laquelle chaque élément est l'identité additive de R est appelée une matrice nulle, ou matrice nulle, et est généralement désignée par $0_{m\times n}$ (0_n).

Exemple 2.4.1. Les matrices nulles dans $M_3(R)$ et $M_{2\times 4}(R)$ sont respectivement :

$$0_3 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \text{ et } 0_{2\times 4} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

La matrice n × n $A = [a_{i,j}]$ sur R telle que $a_{i,i} = 1$ et $a_{i,j} = 0$, pour i = j, est appelée matrice identité d'ordre n sur R et est notée I_n.

Exemple 2.4.2. La matrice identité d'ordre 2 est $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Une matrice m×n $A = [a_{i,j}]$ peut être considérée comme une collection de m vecteurs de lignes, chacun ayant n coordonnées:

$$[a_{1,1}\ a_{1,2}\ \ldots\ a_{1,n}],$$
$$[a_{2,1}\ a_{2,2}\ \ldots\ a_{2,n}],$$
$$\vdots$$
$$[\text{suis},_1 h\ ,_2 h\ \ldots\ \text{suis},_n],$$

ou comme une collection de n vecteurs colonnes, chacun ayant m coordonnées :

$$\begin{bmatrix} a_{1,1} \\ a_{2,1} \\ \vdots \\ \text{suis},1 \end{bmatrix}, \begin{bmatrix} a_{1,2} \\ a_{2,2} \\ \vdots \\ \text{suis},2 \end{bmatrix}, \ldots, \begin{bmatrix} a_{1,n} \\ a_{2,n} \\ \vdots \\ \text{suis},n \end{bmatrix}.$$

Le sous-espace de R^n généré par les vecteurs lignes de A est appelé l'espace des lignes de la matrice A. La dimension de cet espace de lignes est appelée le rang de ligne de A. De même, le sous-espace de R^m généré par les vecteurs colonnes de A est appelé l'espace colonne de A, et sa dimension est la rang de la colonne A.

Il est bien connu que le rang de ligne d'une matrice est égal à son rang de colonne [McC71]. Par conséquent, il n'est pas nécessaire de faire la distinction entre le rang de ligne et le rang de colonne d'une matrice. la valeur commune du rang de ligne et du rang de colonne d'une matrice est appelée simplement le rang de la matrice. Le rang d'une matrice A est ici noté rang(A).

On dit qu'une matrice a un rang maximal si son rang est égal au plus petit du nombre de lignes et colonnes.

Exemple 2.4.3. Considérons les matrices

$$\text{Un} = \begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{matrix} \qquad \text{et } B = \begin{matrix} 1 & 1 & 0 \\ 0 & 0 & 0 \end{matrix},$$

défini sur F2. Alors, puisque rang(A) = 2 = nombre de lignes, A a un rang maximal. La matrice B n'a pas de rang maximal car rang(B) = 1 < nombre de lignes < nombre de colonnes.

On peut définir deux opérations qui donnent à Mn(R) une structure en anneau. Soit A = [ai,j] et B = [bi,j] soient des matrices dans Mm×n(R). La somme de A et B est la matrice m × n C = [ci,j] telle que

$$c_{i,j} = a_{i,j} + b_{i,j} .$$

Maintenant, soit A = [ai,j] une matrice dans Mm×n(R) et B = [bi,j] une matrice dans Mn×p(R). La matrice produit C = [ci,j] = AB est la matrice m × p définie par

$$c_{i,j} = \sum_{k=1}^{n} a_{i,k} b_{k,j} .$$

L'ensemble Mn(R) ainsi que les deux opérations définies ci-dessus constituent un anneau, qui n'est pas commu-
Notez que l'addition de matrices est définie uniquement pour des matrices de même taille, et la le produit est défini entre des matrices telles que le nombre de colonnes de la première matrice soit égal à le nombre de lignes du deuxième.

Exemple 2.4.4. Considérons les matrices A et B de l'exemple précédent. Puis

$$A + B = \begin{matrix} 0 & 1 & 0 \\ 0 & 1 & 1 \end{matrix},$$

et le produit AB n'est pas défini.

On peut également définir une multiplication scalaire qui, avec l'addition matricielle définie ci-dessus, donne $M_{m\times n}(R)$ une structure d'espace vectoriel. Soit α R et soit $A = [a_{i,j}]$ am × n matrice sur R. Ensuite, la multiplication scalaire de α et A, la matrice $C = [c_{i,j}]$, est donnée par

$$c_{i,j} = \alpha a_{i,j} .$$

Si A est une matrice m × n, alors la matrice transposée de A est notée A^T et elle est la matrice n × m matrice dont l'entrée (i, j) est la même que l'entrée (j, i) de la matrice originale A.

Exemple 2.4.5. Soient A et B les matrices suivantes sur R :

$$\text{Un} = \begin{bmatrix} 1 \\ , \\ 3 \end{bmatrix} \quad \text{et } B = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} .$$

Alors,

$$\text{UN}^T = \begin{bmatrix} 1 & 2 & 3 \end{bmatrix} \text{ et } B^T = \begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix} .$$

Pour une matrice A, la sous-matrice $A_{i,j}$ est obtenue en supprimant la ième ligne et la jième colonne.

Exemple 2.4.6. Considérons la matrice B de l'exemple précédent. Alors $B_{1,2} = \begin{bmatrix} 4 & 6 \end{bmatrix}$.

A chaque matrice n × n $A = [a_{i,j}]$ est associé un numéro unique appelé déterminant de A et écrit det(A) ou |A|. Le déterminant de A peut être calculé de manière récursive comme suit :

1. $|A| = a_{1,1}$, si n = 1;
2. $|A| = a_{1,1}a_{2,2} - a_{1,2}a_{2,1}$, si n = 2;
3. $|A| = \sum_{j=1}^{n} (-1)^{1+j} a_{1,j} |A_{1,j}|$, si n > 2.

Il est bien connu qu'une matrice A Mn a un rang n, c'est-à-dire un rang maximal, si et seulement si son le déterminant n'est pas nul [McC71].

Pour une matrice × n A, la matrice adjointe de A est la matrice

$$\text{adj}(A) = [c_{i,j}],$$

où

$$c_{i,j} = (-1)^{i+j} \det(A_{j,i}).$$

Exemple 2.4.7. Considérons les matrices

$$Un = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \quad \text{et } B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix},$$

défini sur F2. Alors, det(A) = 1, det(B) = 0,

$$\mathrm{adj}(A) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad \text{et } \mathrm{adj}(B) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Soit A une matrice × n. A est dite inversible (également non singulière) s'il existe une matrice × n B tel que

$$AB = BA = Dans.$$

Si tel est le cas, la matrice B est déterminée de manière unique par A et est appelée l'inverse de A, noté A^{-1} . L'inverse de A peut être calculé de plusieurs manières. Par exemple,

$$UN^{-1} = \frac{1}{\mathrm{adj}(A).\mathrm{dét}(A)}$$

De plus, A est inversible si et seulement si det(A) = 0 ou, de manière équivalente, rank(A) = n [McC71]. L'ensemble de toutes les matrices inversibles n × n sur R est noté $GL_n(R)$, qui signifie matrices générales groupe linéaire de degré n sur R.

Exemple 2.4.8. La matrice B de l'exemple précédent n'est pas inversible, tandis que la matrice A est inversible et A^{-1} = adj(A).

Notez que les matrices non carrées ne sont pas inversibles. Cependant, elles peuvent être inversibles à gauche ou à droite. Une matrice m × n A est inversible à gauche (à droite) s'il existe une matrice × m B telle que $BA = I_n$ ($AB = I_m$). Une telle matrice B est appelée inverse gauche (droite) de A. On sait que A est gauche (droite) inversible si et seulement si rang(A) = n (rang(A) = m), c'est-à-dire que les colonnes (lignes) de A sont linéairement indépendant.

On dit qu'une matrice est sous forme réduite d'échelons de lignes si et seulement si toutes les conditions suivantes prise:

- la première entrée non nulle de chaque ligne est 1 ;
- chaque ligne a sa première entrée non nulle dans une colonne postérieure à toutes les lignes précédentes ;
- toutes les entrées au-dessus et au-dessous de la première entrée non nulle de chaque ligne sont nulles ;
- toutes les lignes ne contenant que des zéros sont situées en dessous de toutes les autres lignes de la matrice.

On dit que la matrice est sous forme échelonnée en colonnes réduites si sa matrice transposée est sous forme échelonnée en lignes réduites. forme échelonnée.

Exemple 2.4.9. La matrice suivante sur F_2 est sous forme d'échelons de lignes réduits mais n'est pas en forme échelonnée de colonne réduite :

$$\begin{matrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{matrix}$$

2.5 Cartes linéaires

Soient V et W des espaces vectoriels sur le même corps F. Une application $f : V \to W$ est dite linéaire. transformation, application linéaire ou un homomorphisme de V en W, si les conditions suivantes sont vrai:

- $f(v_1 + v_2) = f(v_1) + f(v_2)$, pour tout v_1, v_2 dans V ;
- $f(\alpha v) = \alpha f(v)$, pour tout α dans F et pour tout v dans V .

La première condition stipule que l'addition est préservée sous l'application f. La seconde affirme que la multiplication scalaire est également préservée sous l'application f. Cela équivaut à exiger que il en va de même pour toute combinaison linéaire de vecteurs, c'est-à-dire que pour tout vecteur $v_1, \dots, v_n \in V$, et les scalaires $\alpha_1, \dots, \alpha_n \in F$, l'égalité suivante est vérifiée :

$$f(\alpha_1 v_1 + \cdots + \alpha_n v_n) = \alpha_1 f(v_1) + \cdots + \alpha_n f(v_n).$$

En désignant les éléments nuls des espaces vectoriels V et W respectivement par 0_V et 0_W , il s'ensuit que $f(0_V) = 0_W$ car, en posant $\alpha = 0$ dans la deuxième condition, on obtient :

$$f(0_V) = f(0 \cdot 0_V) = 0f(0_V) = 0_W .$$

Un homomorphisme qui est une application bijective est appelé un isomorphisme linéaire, et s'il existe un isomorphisme de V sur W on dit que V est isomorphe à W, noté VW, et est appelé un isomorphisme de l'espace vectoriel.

Exemple 2.5.1. Soit f : $F_2^3 \to F_2^2$ être la cartographie définie par :

$$f(x, y, z) = (x + y, z).$$

Montrons que f est une application linéaire.

1. Soit v = (v1, v2, v3), w = (w1, w2, w3) F_2^3. Alors

$$\begin{aligned} f(v + w) &= f(v1 + w1, v2 + w2, v3 + w3) \\ &= (v1 + w1 + v2 + w2, v3 + w3) \\ &= (v1 + v2, v3) + (w1 + w2, w3) \\ &= f(v) + f(w). \end{aligned}$$

2. Soit α F2 et v = (v1, v2, v3) F_2^3. Alors

$$\begin{aligned} f(\alpha v) &= f(\alpha v1, \alpha v2, \alpha v3) \\ &= (\alpha v1 + \alpha v2, \alpha v3) \\ &= \alpha(v1 + v2, v3) \\ &= \alpha f(v). \end{aligned}$$

Comme l'addition et la multiplication scalaire sont préservées sous f, on conclut que f est une fonction linéaire. carte.

2.6 Graphiques

Un graphe orienté est une paire ordonnée (V, Γ) où V est appelé l'ensemble des sommets et Γ V × V est appelé l'ensemble des arcs. Si V = le graphe est appelé le graphe vide. Les éléments de V sont appelés les sommets et les éléments de Γ sont appelés arcs. Pour un arc u = (a, b) Γ, a est appelé le sommet initial de u et b le sommet terminal.

Un chemin du graphe (V, Γ) est une suite finie ou infinie d'arcs où le sommet terminal d'un arc est le sommet initial de l'arc suivant. Le nombre d'arcs dans la séquence est appelé la longueur du chemin.

Si = u1u2 · · · un est un chemin du graphe et le sommet terminal de l'arc un est le sommet initial de u1, le chemin est appelé un circuit. Évidemment, s'il existe un circuit alors il existe un chemin de longueur infinie.

Les niveaux de sommets peuvent être définis de manière récurrente comme suit :

- Pour tout sommet a V , si a n'est pas un sommet terminal d'un arc alors le niveau de a est défini être 0;
- Pour tout sommet a dans V , si les niveaux de tous les sommets initiaux des arcs avec a comme sommet terminal ont été définis et le maximum est h alors le niveau de a est défini comme étant h + 1.

Si le niveau de chaque sommet de (V, Γ) est défini et le maximum est , le graphique a un niveau et le le niveau du graphe est défini comme étant . De toute évidence, si chaque sommet du graphe est un sommet isolé (c'est-à-dire, sommet de niveau 0) alors le niveau du graphe est 0. Le niveau du graphe vide est défini à être −1.

Chapitre 3

Transducteurs finis

3.1 Préliminaires sur les transducteurs finis

Un alphabet est un ensemble fini non vide d'éléments où les éléments sont appelés symboles ou lettres. Étant donné un alphabet A, une séquence finie de symboles de A, disons $\alpha = a_0a_1 \cdots a_{l-1}$, est appelé un mot sur A, et l sa longueur qui est notée $|\alpha|$. Le mot vide est un mot de longueur $l = 0$, c'est-à-dire la séquence vide, notée ε. Soit A^n l'ensemble des mots de longueur n, où $n \quad N_0$, alors, par exemple, $A^0 = \{\varepsilon\}$. Soit $A = \quad _{n \geq 0}A^n$ l'ensemble de tous les mots finis et $A^\omega = \{a_0a_1 \cdots a_n \cdots \mid a_i \quad A\}$ est l'ensemble des mots infinis. La concaténation de deux mots dans A , disons $\alpha = a_0a_1 \cdots a_{m-1}$ et $\beta = b_0b_1 \cdots b_{n-1}$, est également un mot dans A de longueur $m + n$ et est noté $\alpha\beta$. De même, si $\alpha = a_0a_1 \cdots a_{m-1} \quad A$ et $\beta = b_0b_1 \cdots b_{n-1} \cdots \quad A^\omega$, alors le la concaténation de α et β est l'élément $a_0a_1 \cdots a_{m-1}b_0b_1 \cdots b_{n-1} \cdots$ de A^ω .

Dans le contexte de ce travail, un transducteur fini (FT) est une machine séquentielle à états finis qui, en tout état donné, lit un symbole d'un ensemble X, produit un symbole d'un ensemble Y et passe à un autre état. Ainsi, étant donné un état initial et une séquence d'entrée finie, un transducteur produit un séquence de sortie de même longueur. La définition formelle d'un transducteur fini est la suivante.

Définition 3.1.1. Un transducteur fini est un quintuple X , Y, S, δ, λ, où :

- X est un ensemble fini non vide appelé alphabet d'entrée ;
- Y est un ensemble fini non vide appelé alphabet de sortie ;

- S est un ensemble fini non vide appelé ensemble des états ;
- $\delta : S \times X \to S$ appelée fonction de transition d'état ; et
- $\lambda : S \times X \to Y$ appelée fonction de sortie.

Tout état de S peut être utilisé comme état initial. Dans ces transducteurs, pour chaque état et chaque entrée, une seule sortie est possible, elles sont donc déterministes.

, Y, S, δ, λ soit un transducteur fini. La fonction de transition d'état δ et la sortie Soit M = X la fonction λ peut être étendue à des mots finis, c'est-à-dire à des éléments de X, de manière récursive, comme suit :

$$\delta(s, \varepsilon) = s \qquad \delta(s, x\alpha) = \delta(\delta(s, x), \alpha)$$

$$\lambda(s, \varepsilon) = \varepsilon \qquad \lambda(s, x\alpha) = \lambda(s, x)\,\lambda(\delta(s, x), \alpha),$$

où s S, x X , et α X .

Exemple 3.1.2. Soit M = {0, 1}, {a, b}, {s1, s2}, δ, λ le transducteur défini par :

$$\delta(s_1, 0) = s_1, \quad \delta(s_1, 1) = s_2, \quad \delta(s_2, 0) = s_1, \quad \delta(s_2, 1) = s_2,$$

$$\lambda(s_1, 0) = a, \quad \lambda(s_1, 1) = a, \quad \lambda(s_2, 0) = b, \quad \lambda(s_2, 1) = b.$$

Ensuite, par exemple,

$$\delta(s_1, 01) = \delta(\delta(s_1, 0), 1) = \delta(s_1, 1) = s_2,$$

$$\lambda(s_1, 01) = \lambda(s_1, 0)\lambda(\delta(s_1, 0), 1) = \text{une}\lambda(s_1, 1) = aa,$$

et

$$\delta(s_1, 0010110) = s_1,$$

$$\lambda(s_1, 0010110) = aaababb.$$

Exemple 3.1.3. Soit M = F_2^2, F_2^3, F_2^2, δ, λ sont le transducteur défini par :

$$\delta(s, x) = As + Bx,$$

$$\lambda(s, x) = Cs + Dx,$$

pour tout s F_2^2, x F_2^2 et où

$$\text{Un} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \quad C = \begin{bmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 1 \end{bmatrix} \quad \text{et } D = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Prendre s = $\begin{matrix} 1 \\ 0 \end{matrix}$ et α = $\begin{matrix} 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \end{matrix}$ Alors,

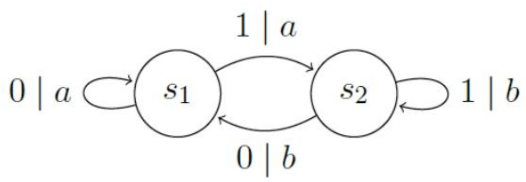
$$\delta(s, \alpha) = \begin{matrix} 0 \\ 0 \end{matrix}$$

$$\lambda(s, \alpha) = \begin{matrix} 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{matrix}$$

M est ce qu'on appelle un transducteur fini linéaire. La définition formelle sera donnée plus loin.

Un transducteur peut être représenté par un diagramme qui est un digramme avec des nœuds et des arcs étiquetés, où des boucles et des arcs multiples sont autorisés. Chaque état du transducteur est représenté par un nœud et chaque arc indique une transition entre des états. L'étiquette de chaque arc est un symbole composé de forme i|o, où i et o représentent respectivement le symbole d'entrée et de sortie. Cette représentation il est utile de traiter à la main les calculs de quelques exemples présentés dans ce chapitre.

Exemple 3.1.4. Le transducteur M défini dans l'exemple 3.1.2 est représenté par le diagramme ci-dessous:



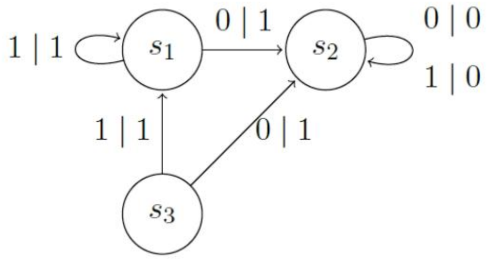
Étant donné ce diagramme, il est assez facile de calculer δ(s, α) et λ(s, α) pour le transducteur, où s S et α X .

Définition 3.1.5. Soient M1 = X , Y1, S1, δ1, λ1 et M2 = X , Y2, S2, δ2, λ2 deux entiers finis transducteurs. Soit s1 S1 et s2 S2. On dit que s1 et s2 sont équivalents, et on note ceci relation par s1 s2, si

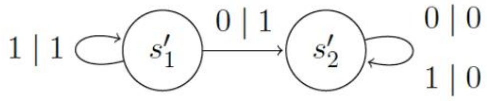
α X , λ1(s1, α) = λ2(s2, α).

Il est évident que si s1 s2 alors x X, δ1(s1, x) δ2(s2, x).

Exemple 3.1.6. Soit M = F2, F2, {s1, s2, s3}, δ, λ le transducteur induit par le diagramme :



et soit M = F2, F2, {s 1 , 2 }, δ , λ soit le transducteur induit par :



Alors

- s2 s 2 , parce que α X , λ(s2, α) = 0 · · · 0 = λ (s 2 , α);
- s1 s3 s 1

Pour prouver que s1 s3, soit α un mot non vide dans F 2 . Alors, soit α est de la forme 0β soit α est de la forme 1β, pour un certain β dans F2 . Dans le premier cas, on a

$$λ(s1, 0β) = λ(s1, 0)λ(δ(s1, 0), β) = 1λ(s2, β),$$

et

$$λ(s3, 0β) = λ(s3, 0)λ(δ(s3, 0), β) = 1λ(s2, β),$$

Il s'ensuit que λ(s1, 0β) = λ(s3, 0β), pour tout β X De même,

$$λ(s1, 1β) = 1λ(s1, β) = λ(s3, 1β),$$

pour tout β X . Par conséquent, α X , λ(s1, α) = λ(s3, α), c'est-à-dire s1 s3. Il est également facile de voir que s1 s 1 .

La définition des états équivalents peut être utilisée pour définir des transducteurs équivalents.

Définition 3.1.7. Soient M1 = X , Y1, S1, δ1, λ1 et M2 = X , Y2, S2, δ2, λ2 deux entiers finis transducteurs. M1 et M2 sont dits équivalents, et on les désigne par M1 M2, si les éléments suivants deux conditions sont simultanément satisfaites :

- s1 S1, s2 S2 : s1 s2;
- s2 S2, s1 S1 : s1 s2.

La relation définit une relation d'équivalence sur l'ensemble des transducteurs finis.

Exemple 3.1.8. Les transducteurs M et M de l'exemple 3.1.6 sont équivalents puisque s1 s3 s 1 et s2 s 2 .

3.2 Concepts sur l'inversibilité

Un concept fondamental dans ce travail est le concept d'injectivité qui est à l'origine de l'inversibilité propriété des transducteurs utilisés à des fins cryptographiques. En fait, il sera présenté deux concepts : le concept d'ω-injectivité et le concept d'injectivité avec un certain retard. Ces deux notions d'injectivité ont été introduites par Tao, qui les a appelées faiblement inversibles et faiblement inversible avec un certain retard, respectivement [Tao09]. Ici, on utilisera des noms qui sont plus naturellement lié à la manière dont ces termes sont utilisés dans d'autres contextes mathématiques.

Définition 3.2.1. Un transducteur fini M = X , Y, S, δ, λ est ω-injectif, si

$$s \quad S, \quad \alpha, \alpha \quad X^{\omega}, \lambda(s, \alpha) = \lambda(s, \alpha) = \quad \alpha = \alpha .$$

C'est-à-dire, pour tout s S et tout α X $^{\omega}$, α peut être déterminé de manière unique par s et λ(s, α).

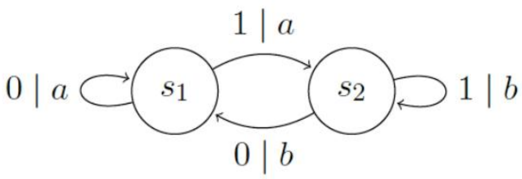
Définition 3.2.2. Un transducteur fini M = X , Y, S, δ, λ est injectif avec un retard τ , ou τ-injectif, avec τ N0, si

$$s \quad S, \quad x, x \quad X , \quad \alpha, \alpha \quad X^{\tau}, \lambda(s, x\alpha) = \lambda(s, x\alpha) = \quad x = x .$$

Autrement dit, pour tout s S, x X, et tout α X τ , x peut être déterminé de manière unique par s et λ(s, xα).

Si un transducteur est injectif avec un délai de 0, étant donné l'état initial et le symbole de sortie, on peut récupérer le symbole d'entrée utilisé. Si un transducteur est injectif avec un certain retard τ , τ N, le premier le symbole d'une séquence d'entrée de longueur $\tau + 1$ peut être récupéré, étant donné l'état initial et le séquence de sortie. Évidemment, si la séquence d'entrée a une longueur $\tau +$, N, on peut récupérer le premiers symboles d'entrée.

Exemple 3.2.3. Le transducteur présenté dans l'exemple 3.1.2 et qui est représenté par le diagramme



est injectif avec un délai de 1. Pour le prouver, il faut calculer la sortie pour chaque état et chaque séquence d'entrée de longueur 2 :

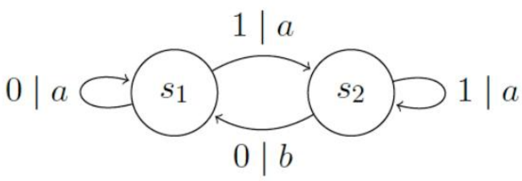
$\lambda(s_1, 00) = aa$,	$\lambda(s_2, 00) = ba$,	$\lambda(s_1, 10) = ab$,	$\lambda(s_2, 10) = bb$,
$\lambda(s_1, 01) = aa$,	$\lambda(s_2, 01) = ba$,	$\lambda(s_1, 11) = ab$,	$\lambda(s_2, 11) = bb$.

À partir de ces résultats, on peut conclure que

$$s \quad \{s_1, s_2\}, \quad x_0x_1, x\ 0x\ 1 \quad \{0, 1\}^2, \lambda(s, x_0x_1) = \lambda(s, x\ 0x\ 1) = \quad x_0 = x_0,$$

ce qui prouve, par définition, que le transducteur est injectif avec un retard de 1. De plus, le transducteur n'est pas injectif avec un délai de 0 (par exemple, $\lambda(s_1, 0) = a = \lambda(s_1, 1)$ et $0 = 1$).

Exemple 3.2.4. Le transducteur M = {0, 1}, {a, b}, {s1, s2}, δ, λ induit par le diagramme



n'est pas injectif avec un délai de 1 puisque, par exemple, $\lambda(s_1, 01) = \lambda(s_1, 11)$ et $0 = 1$.

Soit M = X , Y, S, δ, λ un transducteur fini. Clairement, si M est injectif avec un retard τ N0 alors M est également injectif avec un délai k, pour k ≥ τ , ce qui implique qu'il est également ω-injectif. Tao a prouvé que l'inverse est également vrai [Tao09, Corollaire 1.4.3]. Pour démontrer ce résultat, considérons le graphe GM = (V, Γ) construit à partir de M comme suit. Soit

R = {(δ(s, x), δ(s, x)) | x = x , λ(s, x) = λ(s, x), x, x X , {s S}.

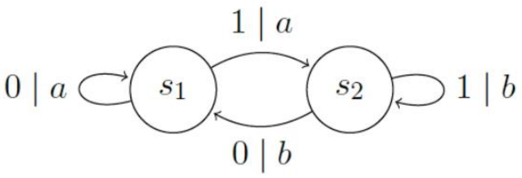
De toute évidence, si (s, s) R alors (s , s) R. Si R = alors GM est le graphe vide. Dans le cas de R = , soit l'ensemble de sommets V de GM le sous-ensemble minimal de S × S satisfaisant les conditions suivantes conditions:

- R V ;
- (s, s) V λ(s, x) = λ(s , x) = (δ(s, x), δ(s , x)) V , où x, x X .

Soit l'ensemble des arcs Γ de GM l'ensemble de tous les arcs ((s, s),(δ(s, x), δ(s , x))) satisfaisant :

- (s, s) V ;
- λ(s, x) = λ(s , x), où x, x X .

Exemple 3.2.5. Considérons le transducteur représenté par le diagramme



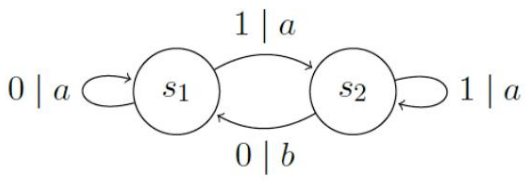
Pour construire le graphe GM, il faut d'abord construire l'ensemble R défini comme ci-dessus. le transducteur un a :

λ(s1, 0) = λ(s1, 1) = a

λ(s2, 0) = λ(s2, 1) = b

alors R = {(δ (s1, 0), δ (s1, 1)) ; (δ (s1, 1), δ (s1, 0)) ; (δ (s2, 0), δ (s2, 1)) ; (δ (s2, 1), δ (s2, 0))} = {(s1, s2),(s2, s1)}. Pour construire l'ensemble de sommets V, il faut l'initialiser comme V = R puis, pour tout paires (s, s) V qui produisent la même sortie pour un certain x, x {0, 1}, (δ(s, x), δ(s , x)) V . Étant donné que x {0, 1}, λ(s1, x) = a et λ(s2, x) = b, les paires dans R ne produisent jamais la même sortie, alors V = R = {(s1, s2),(s2, s1)}. Par conséquent, le graphe GM est composé de deux sommets.

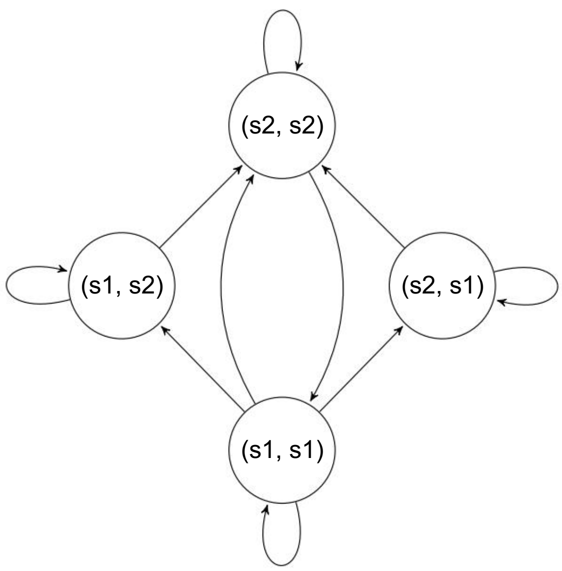
Exemple 3.2.6. Considérons le transducteur M présenté en 3.2.4 induit par le diagramme



Le transducteur produit la sortie a lorsque l'état est s_1 ou lorsque l'état est s_2 et le l'entrée est 1. Par conséquent, puisque R est composé des paires d'états de transition obtenus avec différentes entrées qui produisent la même sortie, $R = \{(\delta(s_1, 0), \delta(s_1, 1)) ; (\delta(s_1, 1), \delta(s_1, 0)) ; (\delta(s_1, 0), \delta(s_2, 1)) ; (\delta(s_2, 1), \delta(s_1, 0))\} = \{(s_1, s_2),(s_2, s_1)\}$.

Soit l'ensemble de sommets V égal à R. Puisque $\lambda(s_1, 0) = \lambda(s_2, 1)$ et $\lambda(s_1, 1) = \lambda(s_2, 1)$, le le sommet (s_1, s_2) a un arc vers le sommet $(\delta(s_1, 0), \delta(s_2, 1)) = (s_1, s_2)$ et un arc vers le sommet $(\delta(s_1, 1), \delta(s_2, 1)) = (s_2, s_2)$. De manière analogue, (s_2, s_1) a un arc vers lui-même et un arc vers le sommet (s_2, s_2). Le nouveau sommet (s_2, s_2) a évidemment un arc vers lui-même et un arc vers (s_1, s_1), puisque $\delta(s_2, 0) = s_1$. Finalement, (s_1, s_1) a un arc vers tous les sommets puisque $\lambda(s_1, 0) = \lambda(s_1, 1)$ et $\delta(s_1, 0) = s_1$ $\delta(s_1, 0) = s_2$.

Le graphe GM est représenté par :



Les théorèmes suivants prouvent que si M est ω-injectif alors M est injectif avec un certain retard τ .

Théorème 3.2.7. Soit $M = \langle X, Y, S, \delta, \lambda \rangle$ un transducteur fini. M est ω-injectif si et seulement si le graphe G_M n'a pas de circuit. De plus, si G_M n'a pas de circuit et son niveau est ρ alors le minimum τ tel que M soit τ -injectif est $\rho + 1$.

Preuve. Supposons que G_M possède un circuit. De la construction du graphe, il existe un chemin $u_1u_2 \cdots u_k$ tel que le sommet initial de u_1 soit dans R et $u_ru_{r+1} \cdots u_k$ est un circuit pour certains r, $1 \leq r \leq k$ (ce qui signifie que le sommet terminal de u_k est le sommet initial de u_r). On a que $\forall i \in \{1, \cdots, k\}$, $u_i = ((s_i, s'_i),(\delta(s_i, x_i), \delta(s'_i, x'_i)))$ et $\lambda(s_i, x_i) = \lambda(s'_i, x'_i)$ pour quelques $x_i, x'_i \in X$. Puisque le sommet initial de u_1 est dans R, il existe $x_0, x'_0 \in X$, $s_0 \in S$ tel que $\lambda(s_0, x_0) = \lambda(s_0, x'_0)$ et $x_0 \neq x'_0$. En prenant $\alpha = x_0x_1 \cdots x_{r-1}x_r \cdots x_kx_r \cdots x_k \cdots$ et $\alpha' = x'_0x'_1 \cdots x'_{r-1}x'_r \cdots x'_kx'_r \cdots x'_k \cdots$, on a que $\alpha \neq \alpha'$ (puisque $x_0 \neq x'_0$) et $\lambda(s_0, \alpha) = \lambda(s_0, \alpha')$, donc M n'est pas ω-injectif (d'après la définition 3.2.1).

Inversement, supposons que G_M n'ait pas de circuit. Alors G_M a un niveau. Soit ρ le niveau du graphe, où $\rho \in \mathbb{N}_0 \cup \{-1\}$. Dans le cas de $R = \emptyset$, il est évident que $\rho = -1$ et M est injectif avec un retard de 0 (= $\rho + 1$) car il n'existe pas de $s \in S$ tel que $\lambda(s, x) = \lambda(s, x')$ et $x \neq x'$.

Dans le cas de $R \neq \emptyset$, pour tout état s_0 de M et pour toute séquence d'entrée $\alpha = x_0x_1 \cdots x_{\rho+1}$ et $\alpha' = x'_0x'_1 \cdots x'_{\rho+1}$, la réduction à l'absurde prouve que $\lambda(s_0, \alpha) = \lambda(s_0, \alpha') \Rightarrow x_0 = x'_0$:

Supposons que $\lambda(s_0, x_0x_1 \cdots x_{\rho+1}) = \lambda(s_0, x'_0x'_1 \cdots x'_{\rho+1})$ et $x_0 \neq x'_0$ pour un certain $s_0 \in S$ et quelques lettres d'entrée. Puisque $\lambda(s_0, x_0x_1 \cdots x_{\rho+1}) = \lambda(s_0, x'_0x'_1 \cdots x'_{\rho+1})$, on a que $\lambda(s_0, x_0) = \lambda(s_0, x'_0)$ et $\lambda(s_i, x_i) = \lambda(s'_i, x'_i)$, $i = 1, 2, \cdots, \rho + 1$. Puisque $x_0 \neq x'_0$, $(s_1, s'_1) = (\delta(s_0, x_0), \delta(s_0, x'_0)) \in R$. De plus, pour tout i, $1 \leq i \leq \rho + 1$, il existe un arc $u_i = ((s_i, s'_i),(s_{i+1}, s'_{i+1}))$. Ainsi $u_1u_2 \cdots u_{\rho+1}$ est un chemin de G_M. Cela signifie que le le niveau du graphique est au moins $\rho + 1$ ce qui contredit le fait que le niveau de G_M est ρ.

Puisque $\lambda(s_0, \alpha) = \lambda(s_0, \alpha') \Rightarrow x_0 = x'_0$, ceci prouve que M est injectif avec un retard $\rho + 1$ (par Définition 3.2.2). □

Exemple 3.2.8. Le transducteur présenté dans l'exemple 3.2.5 a un graphe G_M avec deux sommets, donc G_M a le niveau 0, ce qui signifie que le transducteur est injectif avec un délai de 1 (comme on le voit dans l'exemple 3.2.3). Le graphique du transducteur dans l'exemple 3.2.6 a un circuit, donc ceci le transducteur n'est pas ω-injectif.

Corollaire 3.2.9. Soit M = X , Y, S, δ, λ un transducteur fini. Si M est ω-injectif, alors il y a existe un entier non négatif $\tau \leq \frac{|S|(|S|-1)}{2}$ tel que M soit injectif avec un délai τ .

Preuve. Supposons que M soit ω-injectif. Si GM est le graphe vide alors R = , ce qui signifie que x, x X , s S, x = x = λ(s, x) = λ(s, x). Puisque l'énoncé est logiquement équivalent à x, x X , s S λ(s, x) = λ(s, x) = x = x il résulte, de la définition 3.2.1, que M est injectif avec un retard de 0 et $0 \leq \frac{|S|(|S|-1)}{2}$.

Inversement, supposons que GM ne soit pas le graphe vide. Alors, d'après le théorème précédent, GM a pas de circuits (M est ω-injectif). Si s S tel que (s, s) V , alors (s , s) = (δ(s, x), δ(s, x)) V , puisque x X , λ(s, x) = λ(s, x). Cela donne que s1 = s2 pour tout (s1, s2) V . Ainsi, |V | ≤ |S|(|S| − 1). Il est évident que (s1, s2) V si et seulement si (s2, s1) V , et cela ((s1, s2),(s3, s4)) Γ si et seulement si ((s2, s1),(s4, s3)) Γ. Par conséquent, le nombre de sommets avec le niveau i, 0 ≤ i ≤ ρ, est au moins 2. Puisque le nombre de niveaux est ρ + 1, on a que 2(ρ + 1) ≤ |S|(|S| − 1) ρ + 1 ≤ $\frac{|S|(|S|-1)}{2}$. D'après le théorème 3.2.7, τ = ρ + 1, donc $\tau \leq \frac{|S|(|S|-1)}{2}$. □

Exemple 3.2.10. Du théorème précédent, on peut conclure, encore une fois, que le transducteur M défini dans l'exemple 3.2.4 n'est pas ω-injectif, car il n'est pas injectif avec un délai de 1 et l'ensemble de les états ont une taille de 2 $\tau \leq \frac{|S|(|S|-1)}{2} = \frac{2\times 1}{2} = 1$.

Naturellement, les transducteurs injectifs devraient avoir des inverses d'une certaine sorte. Afin de décrire le concept approprié, la définition suivante introduit une notion d'état inverse d'un État.

Définition 3.2.11. Soit M = X , Y, S, δ, λ et M = Y, X , S , δ , λ soit deux transducteurs finis. Soit s S et s S , alors s inverse s avec un retard τ N0 ou s est un état inverse avec un retard τ de s quand

$$\alpha \quad X^{\omega}, \; \lambda (s , \lambda(s, \alpha)) = \gamma\alpha, \text{ pour certains } \gamma \quad X^{\tau} .$$

Remarque 3.2.12. Dans la définition précédente on peut remplacer X ω par X , mais alors il faut remplacer λ (s , λ(s, α)) = γα par λ (s , λ(s, α)) = γα , où α est constitué du premier |α| − τ caractères de α.

Fondamentalement, en utilisant un état inverse s avec un retard τ d'un état donné s, on peut commencer à récupérer le symboles d'entrée de M après τ symboles lus par M .

La figure ci-dessous donne une représentation schématique du concept d'état inverse avec retard τ ,

où α = x1x2 . . . et λ(s, α) = y1y2 . . . :

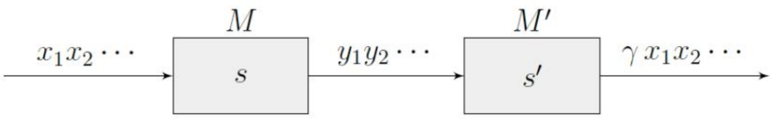
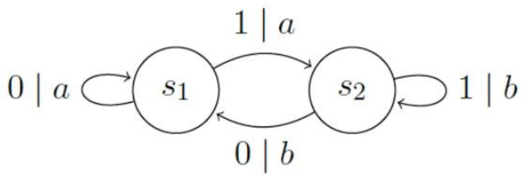


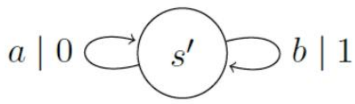
Figure 3.1 : Concept d'état inverse avec retard τ

Exemple 3.2.13. Soit M = {0, 1}, {a, b}, {s1, s2}, δ, λ le transducteur induit par le

diagramme:



et soit M = {a, b}, {0, 1}, {s }, δ , λ soit le transducteur :



L'état s de M inverse les états s1 et s2 de M avec un retard de 1. Pour le prouver, il suffit

pour montrer que, pour tout x1x2 {0, 1}^{2} et pour tout s {s1, s2}, on a

λ (s , λ(s, x1x2)) = xx1, pour un certain x {0, 1},

car cela implique que pour tout α {0, 1} ω et pour tout s {s1, s2},

λ (s , λ(s, α)) = xα, pour certains x {0, 1}.

En utilisant les diagrammes des transducteurs, on obtient facilement

λ (s , λ(s1, 00)) = λ (s , aa) = 00, λ (s , λ(s1, 10)) = λ (s , ab) = 01,

λ (s , λ(s1, 01)) = λ (s , aa) = 00, λ (s , λ(s1, 11)) = λ (s , ab) = 01,

λ (s , λ(s2, 00)) = λ (s , ba) = 10, λ (s , λ(s2, 10)) = λ (s , bb) = 11,

λ (s , λ(s2, 01)) = λ (s , ba) = 10, λ (s , λ(s2, 11)) = λ (s , bb) = 11.

Ceci prouve que s inverse les états s1 et s2 avec un délai de 1.

Définition 3.2.14. Soit M = X , Y, S, δ, λ un transducteur fini. On dit que M est à gauche inversible avec retard τ s'il y a un transducteur M = Y, X , S , δ , λ tel que

s S, s S , s inverse s avec un retard τ.

Le transducteur M est appelé inverse gauche avec retard τ de M.

Il est clair que, dans l'exemple précédent, le transducteur M est un inverse gauche avec un retard 1 de M.

Si M est une inverse à gauche avec un retard τ de M, alors M peut récupérer l'entrée de M avec un retard de τ symboles d'entrée.

Le résultat suivant, prouvé par Tao, établit la relation fondamentale entre l'injectivité d'un transducteur et de l'existence d'un inverse gauche. [Tao09]

Théorème 3.2.15. Un transducteur fini M = X , Y, S, δ, λ est injectif avec retard τ si et seulement si il existe un transducteur fini M = Y, X , S , δ , λ tel que M soit une inverse à gauche avec un retard τ de M.

Plus loin, dans cet ouvrage [Chapitre 4], il sera présenté une condition nécessaire et suffisante à la transducteurs utilisés dans le FAPKC soient inversibles (transducteurs à mémoire). De plus, il on lui montrera une méthode pour construire un inverse gauche d'un transducteur.

3.3 La notion de transducteur fini linéaire

Définition 3.3.1. Si X , Y et S sont des espaces vectoriels sur un corps F et que δ : S × X → S et λ : S × X → Y sont des applications bilinéaires, alors M = X , Y, S, δ, λ est appelé un transducteur fini linéaire (LFT) sur F et la taille de M, notée taille(M), est la dimension de S en tant qu'espace vectoriel.

Exemple 3.3.2. Soit M = F_2^3, F_2^2, F_2^2, δ, λ sont le transducteur défini par :

$$δ(s, x) = (s2 + x1, s1 + x2 + x3),$$

$$λ(s, x) = (s1 + x1 + x3, s2 + x2),$$

pour tout s = (s1, s2) F $_2^2$ et pour tout x = (x1, x2, x3) F $_2^3$. La fonction de transition d'état 5 δ : F_2 2 → F_2 fonction de sortie λ : F → F 2 5 2 et la 2 sont des applications linéaires, par conséquent, M est une application finie linéaire transducteur sur F_2 et la taille de M est $\dim(F_2^2) = 2$. De plus, si l'on considère la norme 5 bases de F_2^2 et F_2^3, ces cartes sont représentées en termes de matrices de la manière suivante

$$\delta(s, x) = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} s_1 & s_2 & x_1 & x_2 & x_3 \end{bmatrix}^T$$

$$= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \mathrm{I} + \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix} x,$$

$$\lambda(s, x) = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} s_1 & s_2 & x_1 & x_2 & x_3 \end{bmatrix}^T$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mathrm{I} + \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} x,$$

Soit M = X , Y, S, δ, λ un transducteur fini linéaire sur un corps F. Si X , Y et S ont des dimensions , m et n, respectivement, alors il existe des matrices A Mn(F), B Mn×(F), C Mm×n(F) et D Mm×(F), tel que, dans les bases appropriées,

$$\delta(s, x) = As + Bx,$$

$$\lambda(s, x) = Cs + Dx,$$

pour tout s S, x X . À partir des calculs effectués sur l'exemple précédent, il est facile de comprendre comment les matrices peuvent être construites à partir des applications δ et λ. Les matrices A, B, C et D sont appelées les matrices structurelles de M, et , m et n sont appelés ses structures paramètres.

Un transducteur fini linéaire tel que C est la matrice nulle (avec les dimensions adéquates) est appelé trivial puisque la sortie de ce transducteur ne dépend que de l'entrée.

3.4 Transducteurs finis avec mémoire

Les transducteurs finis avec mémoire, étant donné un nouveau symbole d'entrée, utilisent les valeurs des entrées passées et, éventuellement, les sorties passées pour calculer un nouveau symbole de sortie. Ce type de transducteurs est la base de les cryptosystèmes analysés. Les clés privées sont composées de deux transducteurs finis avec mémoire, un linéaire et un quasi-linéaire. Transducteurs finis quasi-linéaires, qui seront correctement définis plus loin dans cette section, sont un type spécial de transducteurs finis non linéaires qui ont une partie linéaire et une partie non linéaire de telle sorte que l'inversibilité n'est affectée que par la partie linéaire [Tao09]. La composition de ces deux types de transducteurs produit un transducteur non linéaire, le clé publique. La sécurité des FAPKC repose sur la difficulté de factoriser ce type de transducteurs, ainsi que la difficulté de les inverser.

Pour pouvoir introduire les transducteurs finis linéaires et quasi-linéaires à mémoire, commençons par commencez par définir correctement les transducteurs finis avec mémoire.

Soit X un ensemble non vide et $j \in \mathbb{N}$. On définit $\sigma_j : X^j \times X \rightarrow X^j$ par :

$$\sigma_j((x_1, x_2, \ldots, x_j), x) = (x_2, x_3, \ldots, x_j, x).$$

Définition 3.4.1. Soit $\varphi : X^{h+1} \times Y^k \longrightarrow Y$, avec $h, k \in \mathbb{N}_0$ non simultanément nuls, et X, Y deux ensembles finis non vides. Soit $M_\varphi = \langle X, Y, X^h \times Y^k, \delta_\varphi, \lambda_\varphi \rangle$ soit le transducteur fini tel que, pour tout $x \in X$, $\alpha \in X^h$, $\beta \in Y^k$, les fonctions de transition d'état et de sortie sont données par :

$$\delta_\varphi(< \alpha, \beta >, x) =< \sigma_h(\alpha, x), \sigma_k(\beta, y) >,$$

$$\lambda_\varphi(< \alpha, \beta >, x) = y,$$

où $y = \varphi(\alpha, x, \beta)$ et $< \ldots >$ est utilisé pour désigner les états de ce transducteur. M_φ est appelé le transducteur fini à mémoire (h, k) défini par φ. Si $k = 0$, alors M_φ est dit fini transducteur avec mémoire d'entrée h.

Comme son nom l'indique, un transducteur fini avec mémoire est entièrement défini par sa mémoire (h, k) et par la fonction φ. Notez que δ_φ et λ_φ sont explicitement donnés par φ.

Machine Translated by Google

Ci-dessous, il y a une représentation schématique de la fonction de transition d'état pour ce type de transducteurs. Soit M = X , Y, $X^h \times Y^k$, δ, λ soit un transducteur fini à mémoire d'ordre (h, k), avec h, k N0 non simultanément nuls. Considérons l'état < $x_1, x_2, \ldots, x_h, y_1, y_2, \ldots, y_k$ > $X^h \times Y^k$ et soit y Y la sortie produite par M avec le symbole d'entrée x X . Alors, l'état suivant de M est donné par :

$$< x_1, x_2, \ldots, x_h, y_1, y_2, \ldots, y_k > \xrightarrow{x \mid y} < x_2, \ldots, x_h, x, y_2, \ldots, y_k, y >$$

Notez que l'état actuel de M est composé des h derniers symboles d'entrée et des k derniers symboles de sortie.

Exemple 3.4.2. Soit Mφ le transducteur fini à mémoire d'ordre (3, 2) défini par l'application φ : $F_2^6 \longrightarrow F_2$ avec φ(a, b, c, d, e, f) = ab + c + df. Alors Mφ = F2, F2, F_2^5 , δφ, λφ est tel que

$$\lambda_\varphi(< x_1, x_2, x_3, y_1, y_2 >, x) = \varphi(x_3, x_2, x_1, x, y_2, y_1), \text{ et}$$

$$\delta_\varphi(< x_1, x_2, x_3, y_1, y_2 >, x) =< x_2, x_3, x, y_2, \lambda(< x_3, x_2, x_1, y_2, y_1 >, x) > .$$

5 Prenons s =< 1, 1, 1, 1, 1 > F_2^5 . Alors,

$$\lambda_\varphi(s, 0) = \varphi(1, 1, 1, 0, 1, 1) = 0, \text{ et}$$

$$\delta_\varphi(s, 0) =< 1, 1, 0, 1, 0 > .$$

Dans un transducteur fini avec mémoire d'ordre (h, k), la sortie dépend de l'entrée de courant, la dernières h entrées et les k dernières sorties. Naturellement, il faut définir un état initial. Habituellement, ces les transducteurs sont définis par l'ensemble infini d'équations

$$y_{t+k} = \varphi(x_{t+h}, x_{t+(h-1)}, \ldots, x_{t+1}, x_t , y_{t+(k-1)}, \ldots, y_{t+1}, y_t), \text{ pour } t \geq 0,$$

en commençant par un état initial < $x_0, \ldots, x_{h-1}, y_0, \ldots, y_{k-1}$ >. Notez que, si k = 0, la sortie ne dépend que de l'entrée, c'est-à-dire $y_t = \varphi(x_{t+h}, x_{t+(h-1)}, \ldots, x_{t+1}, x_t)$, pour t ≥ 0, et d'une valeur initiale état < $x_0, \ldots, x_{h-1}$ >.

Par exemple, le transducteur de l'exemple précédent pourrait être défini comme suit. Soit Mφ = F2, F2, F_2^5 , δφ, λφ soit le transducteur fini à mémoire d'ordre (3, 2) défini par

$$y_{t+2} = \varphi(x_{t+3}, x_{t+2}, x_{t+1}, x_t , y_{t+2}, y_{t+1}, y_t) = x_{t+3}x_{t+2} + x_{t+1} + x_t y_{t+1}, \text{ pour } t \geq 0,$$

où $s =< x_0, x_1, x_2, y_0, y_1 >$ est l'état initial du transducteur. Avec ce type de notation nous supposons que

$$y_2y_3y_4 \ldots = \lambda_\varphi(< x_0, x_1, x_2, y_0, y_1 >, x_3x_4, x_5 \ldots)$$

où $x_t, y_t \in F_2$, pour $t \geq 0$.

Exemple 3.4.3. Soit $M = \langle F_2^2, F_2^3, F_2^2 \times (F_2^3)^2, \delta, \lambda\rangle$ soit le transducteur fini avec mémoire de ordre (1, 2) défini par

$$y_{t+2} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix} x_{t+1} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \end{pmatrix} x_t + \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} y_t, \text{ pour } t \geq 0,$$

où $x_t \in F_2^2$, $y_t \in F_2^3$, pour $t \geq 0$, et $< x_0, y_0, y_1 >$ est l'état initial du transducteur.

Prendre $x_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $y_0 = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$, $y_1 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ et $s =< x_0, y_0, y_1 >$. Alors, par exemple,

$$\lambda_s\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Si, dans la définition du transducteur fini à mémoire, $(Y, +)$ est un groupe (pas nécessairement abélien) et la fonction φ est de la forme

$$\varphi = f(x_h, x_{h-1}, \ldots, x_1, x_0) + g(y_{k-1}, \ldots, y_1, y_0),$$

pour certains $f : X^{h+1} \to Y$ et $g : Y^k \to Y$, on dit que M_φ est un transducteur fini séparable avec mémoire, notée $M_{f,g}$. Notez que, en particulier, un transducteur fini avec une mémoire d'entrée uniquement est un transducteur fini séparable.

Exemple 3.4.4. Le transducteur défini dans l'exemple précédent est un transducteur fini séparable, tandis que le transducteur présenté dans l'exemple 3.4.2 n'est pas séparable.

Théorème 3.4.5. Soit Y un groupe noté additivement. Alors, le transducteur fini séparable $M_{f,g} = \langle X, Y, X^h \times Y^k, \delta_{f,g}, \lambda_{f,g}\rangle$ est injectif avec retard τ si et seulement si le transducteur $M_f = \langle X, Y, X^h, \delta_f, \lambda_f\rangle$ est injectif avec un retard τ.

Preuve. Notez que, étant donné sx X h , sy Yk , x X , on peut écrire

$$\lambda f,g(< sx, sy >, x) = f(sx, x) + g(sy).$$

De plus, si α X τ , alors λf,g(< sx, sy >, xα) est simplement une séquence d'éléments comme dans le précédent équation.

Puisque, évidemment, pour tout x, x X

$$f(sx, x) + g(sy) = f(sx, x) + g(sy) \quad f(sx, x) = f(sx, x),$$

on conclut que, pour α X τ ,

$$\lambda f,g(< sx, sy >, x\alpha) = \lambda f,g(< sx, sy >, x\alpha) \quad \lambda f (< sx >, x\alpha) = \lambda f (< sx >, x\alpha).$$

De là découle immédiatement l'affirmation formulée. □

Soit M = X , Y, S, δ, λ un transducteur fini. Dans la section 3.2, il a été démontré que si M est ω-injectif, alors il existe un entier non négatif τ ≤ $\frac{|S|(|S|-1)}{2}$ tel que M soit injectif avec retard τ (Corollaire 3.2.9). Ainsi, pour vérifier si M est ω-injectif, dans le pire des cas, il faut vérifier |S|(|S|−1) si M est τ pour τ = 0, 1, 2, . . . , . Par exemple, soit M = F $\frac{\text{-injectif}}{2}$ $^{2}_{2,2}$ F ^{2} ,(F $^{2}_{2}$)^{3}, δ, λ soit un transducteur fini avec une mémoire d'entrée 3. Puisque |S| = |(F $^{2}_{2}$)^{3} | = 64, pour vérifier si M est injectif, dans dans le pire des cas, il faut vérifier si M est τ-injectif pour τ = 0, 1, . . . , 2016. Si le transducteur a mémoire d'entrée d'ordre 4, alors |S| = |(F $^{2}_{2}$)^{4} | = 256, et le nombre de vérifications s'élève à 32640. Il est facile de voir que le nombre de vérifications augmente de façon exponentielle.

Compte tenu de la structure particulière des transducteurs finis à mémoire, il est plausible que le nombre des vérifications requises est plus faible. Après quelques tests pratiques vérifiant l'injectivité des transducteurs finis avec mémoire et quelques idées partielles pour une preuve (voir annexe A), nous soupçonnons qu'un × Yk , δ, λ fini transducteur avec mémoire M = X , Y, X h est ω-injectif si et seulement s'il existe un entier non négatif τ ≤ h dim(X) tel que M soit injectif avec retard τ .

3.4.1 Transducteurs finis linéaires avec mémoire

Les transducteurs finis linéaires avec mémoire, comme leur nom l'indique, sont associés à des fonctions linéaires. Conformément à la définition 3.4.1, un transducteur fini linéaire avec mémoire est complètement défini par sa mémoire et par la fonction linéaire φ.

Exemple 3.4.6. Le transducteur défini dans l'exemple 3.4.3 est un transducteur fini linéaire avec mémoire, tandis que le transducteur présenté dans l'exemple 3.4.2 n'est pas linéaire.

Exemple 3.4.7. Soit $M = \left(\mathbb{F}_2^2, \mathbb{F}_2^2, (\mathbb{F}_2^2)^3 \times (\mathbb{F}_2^3)^2, \delta, \lambda\right)$ soit le transducteur fini avec mémoire de ordre (3, 2) défini par

$$y_{t+2} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} x_{t+3} + \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} x_{t+1} + \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} x_t + \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} y_{t+1} + \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} y_t, \quad \text{pour } t \geq 0,$$

où $x_t \in \mathbb{F}_2^2$, $y_t \in \mathbb{F}_2^2$, pour $t \geq 0$. Ce transducteur est un transducteur fini linéaire à mémoire.

Soit M un transducteur fini linéaire à mémoire (h, k) défini par $\varphi : X^{h+1} \times Y^k \longrightarrow Y$, avec $h, k \in \mathbb{N}_0$ et $(Y, +)$ un groupe. Puisque φ est une fonction linéaire, on peut toujours la séparer en deux fonctions, $f : X^{h+1} \rightarrow Y$ et $g : Y^k \rightarrow Y$, tel que $\varphi(x_h, \ldots, x_0, y_{k-1}, \ldots, y_0) = f(x_h, \ldots, x_0) + g(y_{k-1}, \ldots, y_0)$. De cette façon, tous les transducteurs finis linéaires sont séparables. Théorème 3.4.5, on peut conclure que l'étude de l'injectivité des transducteurs finis linéaires avec la mémoire peut être réduite à l'étude des LFT avec mémoire en entrée uniquement.

Les transducteurs finis linéaires avec mémoire peuvent être définis comme un système infini d'équations linéaires qui relie la séquence des entrées et des sorties. Soit X l'alphabet d'entrée, Y l'alphabet de sortie alphabet et $h, k \in \mathbb{N}_0$. Soit $S_{h,k}$ l'ensemble des systèmes infinis, dans les variables $(x_t)_{t\geq 0} \in X^{\mathbb{N}_0}$, $(y_t)_{t\geq 0} \in Y$, de la forme :

$$\sum_{j=0}^{h} A_j x_{t+h-j} + \sum_{j=0}^{k+r} B_j y_{t+j} = 0, \text{ pour } t \geq 0,$$

où $r = h \dim(X)$. Tout système infini qui définit un transducteur linéaire avec mémoire d'ordre (h, k) peut être vu comme un système dans $S_{h,k}$, si l'on considère autant de matrices nulles que nécessaire pour « compléter » l'équation générale.

Exemple 3.4.8. Soit $M = \left(\mathbb{F}_2^3, \mathbb{F}_2^3, \mathbb{F}_2^6, \delta, \lambda\right)$ soit le transducteur fini linéaire avec mémoire d'ordre (2, 0) défini par le système infini

$$y_t = A_0x_{t+2} + A_1x_{t+1} + A_2x_t = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} x_{t+2} + \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} x_{t+1} + \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} x_t, \quad \text{pour } t \geq 0.$$

Ce transducteur est le système suivant en $S_{2,0}$:

$$\sum_{j=0}^{h} A_j x_{t+h-j} + \sum_{j=0}^{k+r} B_j y_{t+j} = 0 \qquad \sum_{j=0}^{2} A_j x_{t+2-j} + \sum_{j=0}^{0+2\times 3} B_j y_{t+j} = 0$$

$$\sum_{j=0}^{2} A_j x_{t+2-j} + \sum_{j=0}^{6} B_j y_{t+j} = 0, \text{ pour } t \geq 0,$$

où A_j , pour $j = 0, 1, 2$, sont comme précédemment, $B_0 = I$ et $B_j = 0$, pour $j = 1, 2, \ldots, 6$.

Maintenant, nous définissons deux concepts sur ces systèmes qui seront très utiles à présenter, plus tard dans ce travail, une condition nécessaire et suffisante pour l'injectivité des transducteurs finis linéaires avec mémoire.

Définition 3.4.9. Soit h, k N0 et soit S un système dans $S_{h,k}$. Le rang de S est le rang du matrice des coefficients de x_{t+h} et est notée rang(S), c'est-à-dire rang(S) = rang(A_0).

Exemple 3.4.10. Considérons le transducteur présenté dans l'exemple 3.4.8 et le système infini S associé. Ensuite,

$$\text{rang}(A_0) = \text{rang} \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = 1 = \text{rang}(S).$$

Définition 3.4.11. Un système S dans $S_{h,k}$ est sous forme réduite si les premières lignes de rang (S) de A_0 sont linéairement indépendants et les autres sont nuls.

Notez que la forme réduite d'un système n'est pas unique.

Exemple 3.4.12. Une forme réduite du transducteur $M = \mathbb{F}_2^3, \mathbb{F}_2^3, \mathbb{F}_2^6, \delta, \lambda$ avec mémoire d'entrée 2 présenté dans l'exemple 3.4.8 défini par le système infini

$$y_t = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} x_{t+2} + \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} x_{t+1} + \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} x_t, \quad \text{pour } t \geq 0,$$

s'obtient en additionnant la première ligne à la deuxième :

$$\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} y_t = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} x_{t+2} + \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} x_{t+1} + \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} x_t, \quad \text{pour } t \geq 0.$$

3.4.2 Transducteurs finis quasi-linéaires avec mémoire

Les transducteurs finis quasi-linéaires (QLFT) avec mémoire ont été introduits, autant que nous le sachions, par Renji Tao [Tao09]. L'idée principale derrière le concept de QLFT est d'introduire une sorte de non-linéarité à la définition des transducteurs finis linéaires. Les transducteurs finis linéaires et quasi-linéaires avec mémoire sont faciles à inverser. Dans la composition de ces deux types de transducteurs, le non-la partie linéaire se mélange avec la partie linéaire, ce qui donne un transducteur non linéaire. On ne connaît pas procédure pour inverser les transducteurs non linéaires, par conséquent, on ne peut inverser qu'un transducteur non linéaire en connaissant les facteurs d'origine, dans ce cas les transducteurs linéaires et quasi-linéaires.

Dans son livre, Tao a défini des transducteurs finis quasi-linéaires τ forçant l'entrée $\tau + 1$ la plus récente symboles n'apparaissent que dans la partie linéaire du transducteur. De cette façon, il a pu « étendre » les résultats connus sur l'injectivité des transducteurs finis linéaires.

Définition 3.4.13. Soient $h, k \in \mathbb{N}_0$ et $\tau \in \mathbb{N}_0$ tels que $\tau \leq h$. Soit $M = \langle X, Y, X^h \times Y^k, \delta, \lambda \rangle$ soit un transducteur fini à mémoire d'ordre (h, k). Si M est défini par une équation de la forme

$$y_{t+k} = \sum_{j=0}^{\tau} A_j x_{t+h-j} + f(x_t, x_{t+1}, \ldots, x_{t+h-\tau-1}, y_t, y_{t+1}, \ldots, y_{t+(k-1)}), \text{ pour } t \geq 0,$$

où $f : X^{h-\tau} \times Y^k \to Y$ est une fonction non linéaire, alors on dit que M est une fonction finie τ -quasi-linéaire transducteur (τ-QLFT).

Exemple 3.4.14. Soit $M = \langle \mathbb{F}_2^3, \mathbb{F}_2^3, \mathbb{F}_2^{12}, \delta, \lambda \rangle$ soit le transducteur fini avec une mémoire d'entrée de 2 , 2 , ordre 4 défini par

$$\begin{aligned} y_t &= A_0x_{t+4} + A_1x_{t+3} + A_2x_{t+2} + f(x_t, x_{t+1}) \\ &= \begin{bmatrix} 1&1&0\\0&1&0\\1&0&0 \end{bmatrix} x_{t+4} + \begin{bmatrix} 1&0&0\\0&1&0\\1&1&1 \end{bmatrix} x_{t+3} + \begin{bmatrix} 1&0&0\\0&1&0\\1&0&1 \end{bmatrix} x_{t+2} + f(x_t, x_{t+1}), \text{ pour } t \geq 0, \end{aligned}$$

où $(x_t)_{t\geq 0} \in \mathbb{F}_2^3$, $s = \langle x_0, x_1, x_2, x_3 \rangle \in \mathbb{F}_2^{12}$ est l'état initial du transducteur et f est un fonction non linéaire (par exemple, multiplication par composantes). On peut alors dire que M est un transducteur fini quasi-linéaire 2.

Dans ce qui suit, il est prouvé que le problème de la vérification de l'injectivité des τ-QLFT peut être réduit au problème de la vérification de l'injectivité des transducteurs finis linéaires.

Soient h, k N0 et τ N0 tels que τ ≤ h. Soit $f : X^{h-\tau} \times Y^k \to Y$ soit une fonction non linéaire. Soit $M = X, Y, X^h \times Y^k, \delta, \lambda$ un τ -QLFT défini par

$$y_{t+k} = \sum_{j=0}^{\tau} A_j x_{t+h-j} + f(x_t, x_{t+1}, \ldots, x_{t+h-\tau-1}, y_t, y_{t+1}, \ldots, y_{t+(k-1)}), \text{ pour } t \geq 0.$$

Maintenant, il faut construire un LFT à partir de M comme suit. Soit $M_L = X, Y, X^\tau, \delta_L, \lambda_L$ les transducteur fini linéaire à mémoire d'ordre (τ, 0) défini par

$$y_t = \sum_{j=0}^{\tau} A_j x_{t+\tau-j}, \text{ pour } t \geq 0.$$

Fondamentalement, pour construire ML, nous avons abandonné la partie non linéaire de M.

Théorème 3.4.15. Soit r N0 tel que r ≤ τ . M est inversible avec un retard r si et seulement si ML est inversible avec retard r.

Preuve. Puisque $s =< x_0, \ldots, x_{h-1}, y_0, \ldots, y_{k-1} > X^h \times Y^k$, x, x X , on a :

$$\lambda(s, x) = \lambda(s, x)$$

$$\lambda_L(s_L, x) + f(x_0, \ldots, x_{h-\tau-1}, y_0, \ldots y_{k-1}) = \lambda_L(s_L, x) + f(x_0, \ldots, x_{h-\tau-1}, y_0, .$$

$$\lambda_L(s_L, x) = \lambda_L(s_L, x)$$

où $s_L =< x_{h-\tau}, \ldots, x_{h-1} >$. Alors, x, x X , α, α X on a

$$\lambda(s, x\alpha) = \lambda(s, x\alpha) \qquad \lambda_L(s_L, x\alpha) = \lambda_L(s_L, x\alpha),$$

alors, M est inversible avec un délai r si et seulement si ML est inversible avec un délai r. □

Bien que Tao ait seulement défini et étudié τ-QLFT et son injectivité, définissons un quasi-transducteur fini linéaire.

Définition 3.4.16. Soit h, k N0. Soit $M = X, Y, X^h \times Y^k, \delta, \lambda$ soit un transducteur fini avec mémoire d'ordre (h, k). M est un transducteur fini quasi-linéaire s'il est défini par une équation de la forme

$$y_{t+k} = \sum_{j=0}^{h} A_j x_{t+h-j} + \sum_{j=0}^{k-1} B_j y_{t+j} + f(x_t, x_{t+1}, \ldots, x_{t+(h-1)}, y_t, y_{t+1}, \ldots, y_{t+(k-1)}), \text{ pour } t \geq 0,$$

où $f : X^h \times Y^r \to Y$ est une fonction non linéaire.

Fondamentalement, de cette façon, on peut prendre n'importe quel transducteur fini linéaire et le transformer en un transducteur quasi-linéaire. transducteur fini en ajoutant une fonction non linéaire. Ce fait, à lui seul, nous permet d'élargir la espace de clés privées possibles.

Exemple 3.4.17. Soit $M = F_2^3, F_2^3, F_2^9, \delta, \lambda$ soit le transducteur fini avec une mémoire d'entrée d'ordre défini par :

$$y_t = A_0x_{t+3} + A_1x_{t+2} + A_2x_{t+1} + A_3x_t + f(x_t, x_{t+1}, x_{t+2})$$

$$= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} x_{t+3} + \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} x_{t+2} + \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix} x_{t+1} + \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} x_t + \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} x_{t+2} \cdot x_t,$$

pour $t \geq 0$, où $(x_t)_{t\geq 0}$ F_2^3 et $s_0 =< x_0, x_1, x_2 >$ F_2^3 est l'état initial du transducteur.

Ce transducteur est un transducteur fini quasi-linéaire, uniquement au sens général.

Plus tard, dans ce travail, il sera présenté une condition nécessaire et suffisante pour ces transducteurs être injectif.

Chapitre 4

Inversibilité des transducteurs finis avec Mémoire

Dans le dernier chapitre, nous avons présenté les différents types de transducteurs ainsi que les définitions du transducteur ω-injectif et du transducteur injectif avec retard τ , τ N_0. De plus, il était ont présenté plusieurs résultats liés au problème de la vérification de l'injectivité des transducteurs finis. suggère que l'injectivité des transducteurs est un fait important.

Dans tous les cryptosystèmes, la sécurité repose sur la difficulté de pouvoir inverser le cryptage procédure sans connaître la clé privée. Comme d'habitude dans un système de cryptographie à clé publique, le chiffrement se fait à l'aide de la clé publique, qui dans le cas de FAPKC est un transducteur fini non linéaire qui est la composition des transducteurs de clé privée (un linéaire et un quasi-linéaire). Pour inverser la procédure de cryptage, il faut calculer l'inverse du transducteur de clé publique. Comme dit Jusqu'à présent, on ne connaissait pas de méthode permettant d'inverser les transducteurs finis non linéaires. Cependant, il est possible pour décrypter un texte chiffré si l'on trouve des inverses des transducteurs dans la clé privée (que seule la propriétaire sait) et calculer leur composition. Ce transducteur composé est l'inverse de la transducteur à clé publique utilisé dans le processus de cryptage.

Dans ce chapitre, nous présenterons une procédure permettant de vérifier si un transducteur linéaire avec mémoire est injectif, ainsi qu'une procédure pour calculer son inverse, s'il existe. En fait, pendant la procédure de vérifier l'injectivité, on construit l'inverse du transducteur. De plus, ces résultats seront étendu aux transducteurs finis quasi-linéaires.

4.1 Critère d'inversibilité des LFT avec mémoire

La méthode proposée par Renji Tao pour vérifier l'inversibilité d'un transducteur fini linéaire utilise un paire de transformations qu'il appelle transformations Ra et Rb , appliquées aux équations de la système infini qui définit le transducteur [Tao09]. En gros, les transformations Ra sont utilisé pour obtenir un système équivalent sous forme réduite, et les transformations Rb sont utilisées pour éliminer équations non pertinentes du système infini et réorganiser les autres pour obtenir un nouveau système en la même forme.

Dans ce qui suit, les transformations Ra et Rb seront formalisées ainsi que la procédure pour vérifier la τ-injectivité sur des transducteurs finis linéaires avec mémoire, pour τ N0. De plus, cette La procédure sera illustrée par un exemple.

Pour formaliser la procédure qui vérifie la τ-injectivité des transducteurs finis linéaires, commençons par introduction de deux matrices auxiliaires qui seront utilisées dans les transformations Rb appliquées à la système infini (comme cela sera introduit dans la définition suivante). Soit c, n N où c ≤ n,

$$Je^{+}_{c,n} = \left[\begin{array}{c:c} Moi & 0_{c\times(n-c)} \\ \hdashline 0_{(n-c)\times c} & 0_{n-c} \end{array}\right] \quad \text{et moi} - {}_{c,n} = \left[\begin{array}{c:c} 0_{n-c} & 0_{(n-c)\times c} \\ \hdashline 0_{c\times(n-c)} & Moi \end{array}\right].$$

Fondamentalement, ces matrices nous permettront de « fusionner » les informations nécessaires à partir de deux matrices en une seule. matrice, comme on peut le voir dans l'exemple suivant.

Exemple 4.1.1. Considérons les matrices suivantes :

$$Un = \begin{bmatrix} a_{0,0} & a_{0,1} & a_{0,2} \\ a_{1,0} & a_{1,1} & a_{1,2} \\ a_{2,0} & a_{2,1} & a_{2,2} \end{bmatrix} \quad \text{et } B = \begin{bmatrix} b_{0,0} & b_{0,1} & b_{0,2} \\ b_{1,0} & b_{1,1} & b_{1,2} \\ b_{2,0} & b_{2,1} & b_{2,2} \end{bmatrix}.$$

Pour produire une matrice dont la première ligne est A (et toutes les autres lignes nulles), on peut utiliser $I^{+}_{1,3}$ dans le de la manière suivante :

$$je^{+}_{1,3}A = \left[\begin{array}{c:cc} 1 & 0 & 0 \\ \hdashline 0 & 0 & 0 \\ 0 & 0 & 0 \end{array}\right] \begin{bmatrix} a_{0,0} & a_{0,1} & a_{0,2} \\ a_{1,0} & a_{1,1} & a_{1,2} \\ a_{2,0} & a_{2,1} & a_{2,2} \end{bmatrix} = \begin{bmatrix} a_{0,0} & a_{0,1} & a_{0,2} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Si l'on veut une matrice avec les 2 dernières lignes de B alors il est utile d'utiliser I − : 2,3

$$Je - 2,3B = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} b0,0 & b0,1 & b0,2 \\ b1,0 & b1,1 & b1,2 \\ b2,0 & b2,1 & b2,2 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ b1,0 & b1,1 & b1,2 \\ b2,0 & b2,1 & b2,2 \end{bmatrix}.$$

Pour construire une matrice avec la première ligne de A et les 2 dernières lignes de B on peut procéder comme suit :

$$je^{+}_{1,3}A + I - 2,3B = \begin{bmatrix} a0,0 & a0,1 & a0,2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 \\ b1,0 & b1,1 & b1,2 \\ b2,0 & b2,1 & b2,2 \end{bmatrix} = \begin{bmatrix} a0,0 & a0,1 & a0,2 \\ b1,0 & b1,1 & b1,2 \\ b2,0 & b2,1 & b2,2 \end{bmatrix}.$$

Soit M un transducteur fini linéaire à mémoire d'ordre (h, k), où h, k N0, défini par un système infini d'équations linéaires Sh,k (comme présenté dans la section 3.4.1). La procédure utilisée pour vérifier si M est injectif est formalisé ici comme une transformation Gh,k faisant correspondre l'ensemble Sh,k à lui-même.

Définition 4.1.2. Soit M un transducteur comme précédemment et n N le nombre de lignes du matrice A0. Soit Gh,k : Sh,k → Sh,k la transformation qui affecte à chaque système S Sh,k le système dans Sh,k obtenu de la manière suivante :

Transformation Ra : applique à S une séquence d'opérations élémentaires sur les lignes pour obtenir une équivalence système de carême sous forme réduite ;

Transformation Rb : élimine les équations du système obtenues ci-dessus qui ne dépendent pas sur xt+h ou d'autres entrées ultérieures, c'est-à-dire celles correspondant au n − rang(S) nul lignes de A0, et réorganiser les autres en mettant ensemble les équations qui dépendent de xt+h et ne dépendent pas des entrées suivantes, pour t ≥ 0 (ceci est plus facile à comprendre avec un exemple – voir l'exemple 4.1.4).

Il est facile de voir que, lorsque la matrice A0 a un rang complet, une transformation Gh,k se réduit à une Transformation Ra et on obtient un système équivalent.

Remarque 4.1.3. L'application Gh,k est bien définie, c'est-à-dire que ses images sont dans Sh,k, comme on peut le voir comme suit. Soit h, k N0 et soit S le système dans Sh,k défini par :

$$\sum_{j=0}^{h} Un^{(0)}_{j}\, xt{+}h{-}j + \sum_{j=0}^{k+r} B^{(0)}_{j}\, yt{+}j = 0, \text{ pour } t \geq 0 \text{ et } r = h \dim(xt).$$

Maintenant, laissez

$$\sum_{j=0}^{h} \tilde{A}^{(0)}_j x_{t+h-j} + \sum_{j=0}^{k+r} \tilde{B}^{(0)}_j y_{t+j} = 0, \text{ pour } t \geq 0,$$

soit le système obtenu après la première étape de détermination de $G_{h,k}(S)$, c'est-à-dire après application du Ra transformation. Alors, $G_{h,k}(S)$ est le système

$$\sum_{j=0}^{h} A^{(1)}_j x_{t+h-j} + \sum_{j=0}^{k+r} B^{(1)}_j y_{t+j} = 0, \text{ pour } t \geq 0,$$

où

$$A^{(1)}_j = J_{e+c,m}\tilde{A}^{(0)}_j + J_{e-m-c,m}\tilde{A}^{(0)}_{j+1},$$
$$B^{(1)}_j = J_{e+c,m}\tilde{B}^{(0)}_j + J_{e-m-c,m}\tilde{B}^{(0)}_{j+1},$$

$c = \text{rang}(S)$ et $A^{(0)}_{h+1} = B^{(0)}_{k+r+1} = 0$. On conclut que $G_{h,k}(S) \in S_{h,k}$.

Soit $h, k \in \mathbb{N}_0$ et prenons $S \in S_{h,k}$. Puisque $G_{h,k}$ est une transformation dans $S_{h,k}$, on peut définir $G^{\tau}_{h,k}$ comme le τ -ième itération de $G_{h,k}$, où $\tau \in \mathbb{N}_0$, par

$$G^{0}_{h,k} = id_{S_{h,k}}$$
$$G^{\tau+1}_{h,k} = G^{\tau}_{h,k} \circ G_{h,k}(S)$$

où $id_{S_{h,k}}$ est la transformation d'identité sur $S_{h,k}$ et $G^{\tau}_{h,k} \circ G_{h,k}(S) = G_{h,k}(G_{h,k}(S))$.

Dans l'exemple suivant, il sera illustré comment les transformations $G_{h,k}$ peuvent être utilisées pour vérifier si un transducteur linéaire fini avec mémoire $M = \langle X, Y, X^h \times Y^k, \delta, \lambda \rangle$ est inversible. Que fait-on dans l'exemple est de vérifier s'il existe $\tau \in \mathbb{N}_0$ tel que $\forall s \in S, \forall x \in X, \forall \alpha \in X^{\tau}$, x est unique déterminé par s et $\lambda(s, x\alpha)$.

Soit $M = \langle X, Y, X^h, \delta, \lambda \rangle$ soit un transducteur fini linéaire avec une mémoire d'entrée d'ordre h. Pour illustrer la procédure, il sera utilisé un transducteur avec mémoire d'entrée uniquement, car, en plus d'être plus simple, le problème du test d'injectivité des transducteurs linéaires avec mémoire peut être réduit à le problème de la vérification de l'injectivité des transducteurs linéaires avec mémoire d'entrée uniquement (section 3.4.1). De plus, rappelons que, puisque M est un transducteur avec une mémoire d'entrée h, si M est τ -injectif alors $\tau \leq h \dim(X)$.

Soit M un transducteur comme précédemment. Soit $x_h x_{h+1} x_{h+2} \ldots$ une séquence d'entrée, où $(x_t)_{t \geq h} \in X^{\omega}$, et $s = \langle x_0, x_1, \ldots, x_{h-1} \rangle \in X^h$ être l'état initial du transducteur. Ensuite, la sortie séquence du transducteur est donné par $y_0y_1y_2 \ldots = \lambda(s, x_hx_{h+1}x_{h+2} \ldots)$, où $(y_t)_{t\geq 0} \in Y$. Dans la l'exemple suivant, pour vérifier si le transducteur M est injectif, c'est-à-dire s'il est possible de récupérer le premier symbole d'entrée, il sera traité séquentiellement comme suit :

- Tout d'abord, on vérifie si, étant donné s et y_0, x_h est déterminé de manière unique par eux. Si c'est vrai, le transducteur est inversible avec un délai de 0 ;
- Sinon, on vérifie si x_h est déterminé de manière unique par s, y_0 et y_1. Dans ce cas, le transducteur est inversible avec un délai de 1 ;
- Ceci peut être continué jusqu'à ce que l'on vérifie si x_h est déterminé de manière unique par s et $y_0, y_1, \ldots, y_{h \dim(X)}$. Si cela est vrai, le transducteur est inversible avec un retard $h \dim(X)$ et x_h peut être récupéré. Dans le cas contraire, on peut conclure que le transducteur n'est pas injectif.

En fait, vérifier si x_h est déterminé de manière unique par s et $y_0, y_1, \ldots, y_\tau$ équivaut à vérifier si le la matrice A_0 du système infini dans la τ-ième transformation $G_{h,k}$ a le rang complet.

Notez que, après avoir atteint un système où la matrice A_0 a le rang complet, si l'on continue à appliquer Transformations $G_{h,k}$, on obtiendra des systèmes équivalents, donc la procédure se termine lorsque la matrice A_0 a un rang complet. Cela signifie que le transducteur M est injectif avec un retard égal à le nombre de transformations $G_{h,k}$ appliquées, ou lorsque la limite de la τ-injectivité est atteinte.

Exemple 4.1.4. Soit $M = \langle \mathbb{F}_2^3, \mathbb{F}_2^3, \mathbb{F}_2^6, \delta, \lambda \rangle$ soit le transducteur fini linéaire avec une mémoire d'entrée de 2, ordre 2 défini par le système infini

$$y_t = A_0x_{t+2} + A_1x_{t+1} + A_2x_t = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} x_{t+2} + \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} x_{t+1} + \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} x_t, \quad \text{pour } t \geq 0,$$

où $(x_t)_{t\geq 0} \in \mathbb{F}_2^3$ et $s_0 = \langle x_0, x_1 \rangle$ est l'état initial du transducteur. Soit $(x_t)_{t\geq 2} \in \mathbb{F}_2^3$ être une séquence d'entrée et considérer $(y_t)_{t\geq 0} = \lambda(s_0,(x_t)_{t\geq 2})$.

Notez que les deuxième et troisième colonnes de A_0 sont nulles. Par conséquent, y_0 ne contient aucun informations sur les deuxième et troisième composantes de x_2. Par conséquent, x_2 n'est pas uniquement déterminé par y_0 et s_0, c'est-à-dire que le transducteur n'est pas inversible avec un délai de 0.

L'ajout de la connaissance de y_1, par la procédure présentée précédemment, permet de déterminer de manière unique x_2. La première étape consiste à appliquer au système une séquence d'opérations élémentaires sur les lignes pour obtenir une système équivalent sous forme réduite, c'est-à-dire appliquer une transformation R_a . Ceci peut être obtenu (comme cela a été fait dans l'exemple 3.4.12) en ajoutant la première ligne à la deuxième :

$$\begin{bmatrix}1&0&0\\1&1&0\\0&0&1\end{bmatrix} y_t = \begin{bmatrix}1&0&0\\0&0&0\\0&0&0\end{bmatrix} x_{t+2} + \begin{bmatrix}1&0&0\\1&1&0\\0&1&1\end{bmatrix} x_{t+1} + \begin{bmatrix}1&0&0\\1&1&0\\0&0&0\end{bmatrix} x_t \text{ , pour } t \geq 0.$$

Ensuite, étendons le nouveau système de la manière suivante :

$$\begin{aligned}
\begin{bmatrix}1&0&0\\1&1&0\\0&0&1\end{bmatrix} y_0 &= \begin{bmatrix}1&0&0\\0&0&0\\0&0&0\end{bmatrix} x_2 + \begin{bmatrix}1&0&0\\1&1&0\\0&1&1\end{bmatrix} x_1 + \begin{bmatrix}1&0&0\\1&1&0\\0&0&0\end{bmatrix} x_0\\
\begin{bmatrix}1&0&0\\1&1&0\\0&0&1\end{bmatrix} y_1 &= \begin{bmatrix}1&0&0\\0&0&0\\0&0&0\end{bmatrix} x_3 + \begin{bmatrix}1&0&0\\1&1&0\\0&1&1\end{bmatrix} x_2 + \begin{bmatrix}1&0&0\\1&1&0\\0&0&0\end{bmatrix} x_1\\
&\vdots\\
\begin{bmatrix}1&0&0\\1&1&0\\0&0&1\end{bmatrix} y_t &= \begin{bmatrix}1&0&0\\0&0&0\\0&0&0\end{bmatrix} x_{t+2} + \begin{bmatrix}1&0&0\\1&1&0\\0&1&1\end{bmatrix} x_{t+1} + \begin{bmatrix}1&0&0\\1&1&0\\0&0&0\end{bmatrix} x_t\\
\begin{bmatrix}1&0&0\\1&1&0\\0&0&1\end{bmatrix} y_{t+1} &= \begin{bmatrix}1&0&0\\0&0&0\\0&0&0\end{bmatrix} x_{t+3} + \begin{bmatrix}1&0&0\\1&1&0\\0&1&1\end{bmatrix} x_{t+2} + \begin{bmatrix}1&0&0\\1&1&0\\0&0&0\end{bmatrix} x_{t+1}\\
&\vdots
\end{aligned}.$$

Il y a 2 équations ($3 - \text{rang}(S)$) qui ne dépendent pas de x_2 et peuvent donc être rejetées dans le but d'obtenir x_2 à partir de s_0 et y_0y_1. L'étape suivante consiste à éliminer ces équations et de réorganiser les autres en mettant ensemble les équations qui dépendent de x_{t+2} et ne le font pas dépendent des entrées suivantes, c'est-à-dire en appliquant une transformation R_b . Pour ce faire, pour deux équations matricielles consécutives, réaffecter les lignes en mettant ensemble les 1 premières ($\text{rang}(S)$) ligne de la première équation et les 2 dernières lignes ($3 - \text{rang}(S)$) de la deuxième équation. Le résultat de cette procédure est le système suivant :

$$\begin{bmatrix}0&0&0\\1&1&0\\0&0&1\end{bmatrix} y_{t+1} + \begin{bmatrix}1&0&0\\0&0&0\\0&0&0\end{bmatrix} y_t = \begin{bmatrix}1&0&0\\1&1&0\\0&1&1\end{bmatrix} x_{t+2} + \begin{bmatrix}1&0&0\\1&1&0\\0&0&0\end{bmatrix} x_{t+1} + \begin{bmatrix}1&0&0\\0&0&0\\0&0&0\end{bmatrix} x_t, \quad \text{pour } t \geq 0.$$

La matrice des coefficients de x_{t+2} est inversible, c'est-à-dire que la matrice A_0 de $G_{2,0}(S)$ a un rang complet, donc, en utilisant ce nouveau système, x_2 est déterminé de manière unique par s_0, y_0 et y_1, c'est-à-dire que le transducteur est injectif avec retard 1.

4.2 Inverses des LFT avec mémoire

La section précédente comprenait une condition nécessaire et suffisante pour un transducteur fini linéaire $M = \langle X, Y, X^h \times Y^k, \delta, \lambda \rangle$, avec mémoire d'ordre (h, k), $h, k \in \mathbb{N}_0$, défini par un système $S \in S_{h,k}$, doit être inversible avec un délai $\tau \leq h \dim(X)$, étant entendu que la matrice A_0 dans $G^{\tau}_{h,k}(S)$ doit avoir un rang maximal.

Dans cette section, il sera montré comment construire un inverse de transducteurs finis linéaires avec mémoire d'ordre (h, k), dans le cas où il y en aurait une. Afin de pouvoir démontrer les résultats associés aux inverses, introduisons d'abord les lemmes suivants.

Lemme 4.2.1. Soit $h, k \in \mathbb{N}_0$ et soit S un système dans $S_{h,k}$, où la matrice A_0 a n lignes, $n \in \mathbb{N}$. Alors :

P1 S implique $G_{h,k}(S)$, c'est-à-dire que si $(x_t, y_t)_{t\geq 0}$ est une solution de S, alors c'est aussi une solution de $G_{h,k}(S)$;

P2 si $(x_t, y_t)_{t\geq 0}$ est une solution de $G_{h,k}(S)$ alors $(x_t, y_t)_{t\geq 1}$ est une solution de S.

Preuve. La propriété P1 est assez évidente puisque $G_{h,k}(S)$ est obtenu à partir de S par une suite de opérations élémentaires sur les lignes, qui préservent l'équivalence des systèmes, puis certaines équations de la système sont supprimés. Ainsi, l'ensemble des solutions de S est un sous-ensemble des solutions de $G_{h,k}(S)$.

Pour prouver la deuxième propriété, notez que $G_{h,k}(S)$ est obtenu à partir d'un système équivalent à S par en supprimant un sous-ensemble de ses n premières équations. Alors, si $(x_t, y_t)_{t\geq 0}$ est une solution de $G_{h,k}(S)$, elle est aussi une solution du système obtenue en supprimant toutes les n premières équations, qui est ici notée par $G_{h,k}(S)'$. S est un système défini par $\sum_{j=0}^{h} A_j x_{t+h-j} + \sum_{j=0}^{k+r} B_j y_{t+j} = 0$, pour $t \geq 0$, ou de manière équivalente, Ah Ah−1 Ah−2 . . . A0 0 0 0 . . . x0

S : 0 Ah Ah−1 . . . A1 A0 0 0 . . . x1 +

0 0 Ah . . . A2 A1 A0 0 . . . x2

⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮

B0 B1 B2 . . . Bk+r 0 0 0 . . . y0

0 B0 B1 . . . Bk+r−1 Bk+r 0 0 . . . y1 .

0 0 B0 . . . Bk+r−2 Bk+r−1 Bk+r 0 . . . y2

⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮

Le système Gh,k(S) , obtenu à partir de S en supprimant les n premières équations, est défini par :

x0

0 Ah Ah−1 . . . A1 A0 0 0 . . . x1

G(S) : 0 0 Ah . . . A2 A1 A0 0 . . . x2 +

⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮

y0

0 B0 B1 . . . Bk+r−1 Bk+r 0 0 . . . y1

0 0 B0 . . . Bk+r−2 Bk+r−1 Bk+r 0 . . . y2

⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮

ou, $0x0 + \sum_{j=0}^{h} Aj\, xt+h−j + 0y0 + \sum_{j=0}^{k+r} Bj\, yt+j = 0$, pour t ≥ 1. Supposons que (xt , yt)t≥0 est un solution de Gh,k(S) (également une solution de Gh,k(S)), alors :

$$\sum_{j=0}^{h} Aj\, xt+h−j + \sum_{j=0}^{k+r} Bj\, yt+j = 0, t \geq 1 \quad \sum_{j=0}^{h} Aj\, xt+1+h−j + \sum_{j=0}^{k+r} Bj\, yt+1+j = 0, t \geq 0$$

(xt+1, yt+1)t≥0 = (xt , yt)t≥1 est une solution de S.

□

Cette propriété peut naturellement être étendue à Gτ pour τ ≥ 0, de la manière suivante : h,k,

Lemme 4.2.2. Soit h, k N0 et soit S le système dans Sh,k. Alors :

P1 S implique Gτ h,k(S), c'est-à-dire que si (xt , yt)t≥0 est une solution de S, alors c'est aussi une solution de Gτ h,k(S) ;

P2 si (xt , yt)t≥0 est une solution de Gτ h,k(S) alors (xt , yt)t≥τ est une solution de S.

Dans le résultat suivant, il est montré une manière d'obtenir l'inverse d'un transducteur fini linéaire τ-injectif avec mémoire d'ordre (h, 0).

Théorème 4.2.3. Soit N. Soit M = X , Y, X ^{h}, δ, λ = F $_{2}$, F $_{2}$, F $_{2}^{h}$, δ, λ le fini linéaire transducteur à mémoire d'ordre (h, 0) défini par le système infini :

$$S : \sum_{j=0}^{h} A^{(0)}_j x_{t+h-j} + \sum_{j=0}^{l} B^{(0)}_j y_{t+j} = 0, \text{ pour } t \geq 0,$$

où r = h, A (0) j M , B = I et B = 0 pour 0 < j ≤ r. Si Gτ 0 h,0 j (S) est le système

$$\sum_{j=0}^{h} A^{(\tau)}_j x_{t+h-j} + \sum_{j=0}^{l} B^{(\tau)}_j y_{t+j} = 0, \text{ pour } t \geq 0,$$

alors M est inversible avec retard τ si et seulement si A 0 (τ) est une matrice inversible. Soit L l'inverse matrice de A (τ) 0 . Soit M = Y, X , Y τ × X ^{h}, δ , λ = F $_{2}$, F $_{2}$, F $_{2}^{(\tau+h)}$, δ , λ soit la fonction linéaire transducteur fini à mémoire d'ordre (τ, h) obtenu en multipliant, à gauche, les deux côtés de $G^{\tau}_{h,0}$ (S) par L :

$$\sum_{j=0}^{h} LA^{(\tau)}_j x_{t+h-j} + \sum_{j=0}^{l} LB^{(\tau)}_j y_{t+j} = 0, \text{ pour } t \geq 0.$$

Alors, M est une inverse gauche avec retard τ de M, et M est une inverse gauche avec retard τ de M .

Preuve. Tout d'abord, notons que, dans le transducteur M , LA(τ) 0 (τ) est la matrice identité et B = 0 pour j j > τ . Pour construire M , l'inverse de M, il faut voir le transducteur « à l'envers », c'est à dire c'est-à-dire, voir l'entrée comme sortie et vice versa. Puisque M est injectif avec un retard τ , il faudra le information de $(y_i)_{0\leq i\leq\tau}$ pour inverser le transducteur, par conséquent, l'inverse aura une mémoire d'entrée d'ordre τ . De plus, le transducteur inverse aura une mémoire de sortie h, la mémoire d'entrée étant de M.

Pour prouver que M est une inverse à gauche avec retard τ de M, il faut démontrer que s X ^{h}, s Y τ × X h : α X $^{\omega}$, λ (s , λ(s, α)) = γα pour certains γ X τ (par la Définition 3.2.11 et la Définition 3.2.14). Soit s =< xτ , xτ+1, . . . , xτ+h−1 > un état générique de M. On démontrera que tout de M de la forme < y0, y1, . . . , yτ−1, x0, x1, . . . , xh−1 > inverse s avec retard τ état s , où x0, x1, . . . , xτ−1 sont des éléments arbitraires dans X (remarquez que les valeurs de xτ , xτ+1, . . . , xτ+h−1 sont en s) et

$$y_0y_1 \ldots y_{\tau-1} = \lambda(< x_0, x_1, \ldots , x_{h-1} >, x_hx_{h+1} \ldots x_{h+\tau-1}).$$

Considérons maintenant la séquence d'entrée $(x_t)_{t\geq h+\tau}$ et

$$(y_t)_{t\geq\tau} = \lambda(< x_\tau , x_{\tau+1}, \ldots , x_{\tau+h-1} >,(x_t)_{t\geq h+\tau}).$$

Machine Translated by Google

À partir des deux dernières équations, on a $(x_t)_{t\geq 0} = \lambda(< x_0, x_1, \ldots, x_{h-1} >,(x_t)_{t\geq h})$. Cela signifie que $(x_t)_{t\geq 0}$ et $(y_t)_{t\geq 0}$ satisfont le système d'équations S qui définit le transducteur M.

Alors, d'après la propriété P1 du lemme 4.2.2, $(x_t)_{t\geq 0}$ et $(y_t)_{t\geq 0}$ satisfont également le système $G^{\tau}_{h,0}$ (S).

Par conséquent, puisque le système qui définit le transducteur M est obtenu à partir de $G^{\tau}_{h,0}$ (S) par en multipliant ceci par la matrice L, $(x_t)_{t\geq 0}$ et $(y_t)_{t\geq 0}$ satisfont également le système de M , c'est,

$$(x_t)_{t\geq h} = \lambda (< y_0, y_1, \ldots, y_{\tau-1}, x_0, x_1, \ldots, x_{h-1} >,(y_t)_{t\geq \tau})$$

$$(x_t)_{t\geq h} = \lambda (< y_0, y_1, \ldots, y_{\tau-1}, x_0, x_1, \ldots, x_{h-1} >, \lambda(< x_\tau , x_{\tau+1}, \ldots, x_{\tau+h-1} >,(x_t)_{ t\geq h+\tau})).$$

Ensuite, il a été prouvé que, pour $\alpha = (x_t)_{t\geq h+\tau}$ X^ω, (s , $\lambda(s, \alpha)) = \gamma\alpha$ où $\gamma = (x_t)_{h\leq t<h+\tau}$ λ X^τ. Par conséquent, M est une inverse à gauche avec un retard τ de M.

Pour prouver la deuxième affirmation selon laquelle M est une inverse à gauche avec un retard τ de M , laissons $=< y_0, y_1, \ldots, y_{\tau-1}$, $x_{h-1} >$ un état générique de M et $s =< x_\tau , x_{\tau+1}, \ldots, x_{\tau+h-1} >$ un état de S, $x_0, x_1, \ldots,$ où $x_h, x_{h+1} \ldots, x_{\tau+h-1}$ sont des éléments arbitraires dans X (remarquez que les symboles $x_\tau , x_{\tau+1}, \ldots, x_{h-1}$). Il sera démontré que s inverse s sont dans s avec retard τ .

Considérons la séquence d'entrée $(y_t)_{t\geq \tau}$ Y^ω , alors

$$(x_t)_{t\geq h} = \lambda (< y_0, \ldots, y_{\tau-1}, x_0, \ldots, x_{h-1} >,(y_t)_{t\geq \tau}).$$

Cela signifie que $(x_t)_{t\geq 0}$ et $(y_t)_{t\geq 0}$ satisfont le système infini qui définit le transducteur M et, par conséquent, satisfont le système $G^{\tau}_{h,0}$ (S). Alors, d'après la propriété P2 du lemme 4.2.2, $(x_t)_{t\geq \tau}$ et $(y_t)_{t\geq \tau}$ satisfont le système associé au transducteur M, c'est-à-dire,

$$\begin{aligned}(y_t)_{t\geq \tau} &= \lambda(< x_\tau , x_{\tau+1}, \ldots, x_{\tau+h-1} >,(x_t)_{t\geq \tau+h}) \\ &= \lambda(s,(x_t)_{t\geq \tau+h}).\end{aligned}$$

De cette façon, on peut récupérer la séquence d'entrée $(y_t)_{t\geq \tau}$ Y^ω donc, s est un état inverse de s .
De plus, M est une inverse à gauche avec un retard τ de M . □

Bien que le dernier résultat ne montre que la construction d'inverses de transducteurs finis linéaires avec mémoire d'ordre (h, 0), le résultat peut être étendu aux transducteurs à mémoire (h, k). En fait, la formule du transducteur inverse est la même que celle présentée précédemment, et la preuve est analogique.

Comme on le voit dans le dernier théorème, l'inverse d'un transducteur fini linéaire est construit pendant la procédure de vérification de son injectivité.

Exemple 4.2.4. Soit $M = \langle \mathbb{F}_2^3, \mathbb{F}_2^3, \mathbb{F}_2^6, \delta, \lambda \rangle$ soit le transducteur infini avec mémoire (2, 0) défini par le système infini

$$y_t = A_0x_{t+2} + A_1x_{t+1} + A_2x_t = \begin{bmatrix}1&0&0\\1&0&0\\0&0&0\end{bmatrix} x_{t+2} + \begin{bmatrix}1&0&0\\0&1&0\\0&1&1\end{bmatrix} x_{t+1} + \begin{bmatrix}1&0&0\\0&1&0\\0&0&0\end{bmatrix} x_t\ , \quad \text{pour } t \geq 0,$$

où x_t , x_{t+1}, $x_{t+2} \in \mathbb{F}_2^3$ et $s_0 = \langle x_0, x_1 \rangle$ est l'état initial du transducteur.

Dans l'exemple 4.1.4, le système infini $G_{2,0}(S)$ a été calculé , qui a le rang complet :

$$\begin{bmatrix}0&0&0\\1&1&0\\0&0&1\end{bmatrix} y_{t+1} + \begin{bmatrix}1&0&0\\0&0&0\\0&0&0\end{bmatrix} y_t = \begin{bmatrix}1&0&0\\1&1&0\\0&1&1\end{bmatrix} x_{t+2} + \begin{bmatrix}1&0&0\\1&1&0\\0&0&0\end{bmatrix} x_{t+1} + \begin{bmatrix}1&0&0\\0&0&0\\0&0&0\end{bmatrix} x_t\ , \quad \text{pour } t \geq 0.$$

M est donc inversible. Pour obtenir le transducteur inverse de M il suffit de multiplier, sur à gauche, l'équation précédente par la matrice inverse de A_0. Puisque

$$\begin{bmatrix}1&0&0\\1&1&0\\1&1&1\end{bmatrix} \begin{bmatrix}1&0&0\\1&1&0\\0&1&1\end{bmatrix} = \begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix},$$

on peut obtenir le transducteur inverse en multipliant le système infini $G_{2,0}(S)$ par $L = \begin{bmatrix}1&0&0\\1&1&0\\1&1&1\end{bmatrix}$:

$$\begin{bmatrix}0&0&0\\1&1&0\\1&1&1\end{bmatrix} y_{t+1} + \begin{bmatrix}1&0&0\\1&0&0\\1&0&0\end{bmatrix} y_t = \begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix} x_{t+2} + \begin{bmatrix}1&0&0\\0&1&0\\0&1&0\end{bmatrix} x_{t+1} + \begin{bmatrix}1&0&0\\1&0&0\\1&0&0\end{bmatrix} x_t\ , \quad \text{pour } t \geq 0.$$

Alors, le transducteur inverse de M est le transducteur $M^* = \langle \mathbb{F}_2^3, \mathbb{F}_2^3, \mathbb{F}_2^9, \delta^*, \lambda^* \rangle$ avec mémoire de ordre (1, 2) défini par le système infini

$$x_{t+2} = \begin{bmatrix}0&0&0\\1&1&0\\1&1&1\end{bmatrix} y_{t+1} + \begin{bmatrix}1&0&0\\1&0&0\\1&0&0\end{bmatrix} y_t + \begin{bmatrix}1&0&0\\0&1&0\\0&1&0\end{bmatrix} x_{t+1} + \begin{bmatrix}1&0&0\\1&0&0\\1&0&0\end{bmatrix} x_t\ , \quad \text{pour } t \geq 0.$$

Rappelons que les symboles d'entrée de ce transducteur sont en Y et les symboles de sortie en X.

4.3 Critère d'inversibilité et inverses des QLFT avec mémoire

Comme indiqué précédemment, Renji Tao a défini un transducteur fini quasi-linéaire de manière à ce que les résultats connus sur l'inversibilité des transducteurs finis linéaires pourrait être étendue [Section 3.4.2]. Soit $\tau \in \mathbb{N}$ et $r \in \mathbb{N}_0$ tel que $r \leq \tau$. Comme le prouve le théorème 3.4.15, un transducteur fini τ -quasi-linéaire est inversible avec délai r si et seulement si la partie linéaire du transducteur est inversible avec délai r. Ainsi, la procédure présentée précédemment peut être appliquée aux transducteurs finis quasi-linéaires.

Dans l'exemple suivant, la procédure permettant de vérifier l'injectivité dans un système fini quasi-linéaire sera présentée. transducteur avec mémoire. Cette procédure ne peut être appliquée qu'à la partie linéaire du transducteur mais, pour pouvoir construire son inverse, il faudra l'appliquer à l'ensemble du transducteur.

Exemple 4.3.1. Soit $M = \langle \mathbb{F}_2^3, \mathbb{F}_2^3, \mathbb{F}_2^{12}, \delta, \lambda \rangle$ soit un transducteur fini 2-quasi-linéaire avec entrée 2 , 2 , mémoire d'ordre 4 présentée dans l'exemple 3.4.14 et définie par :

$$
\begin{aligned}
y_t &= A_0x_{t+4} + A_1x_{t+3} + A_2x_{t+2} + f(x_t , x_{t+1}) \\
&= \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} x_{t+4} + \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} x_{t+3} + \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} x_{t+2} + \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} x_{t+1} \cdot x_t \quad , \text{ pour } t \geq 0,
\end{aligned}
$$

où $(x_t)_{t\geq 0} \in \mathbb{F}_2^3$, $s_0 =< x_0, x_1, x_2, x_3 > \in \mathbb{F}_2^{12}$ est l'état initial du transducteur et · représente pour la multiplication par composantes. Soit $(x_t)_{t\geq 4}$ une séquence d'entrée et considérons $(y_t)_{t\geq 0} = \lambda(s_0,(x_t)_{t\geq 4})$.

Notez que la troisième colonne de A_0 est nulle. Par conséquent, y_0 ne contient aucune information sur la troisième composante de x_4. Par conséquent, x_4 n'est pas uniquement déterminé par y_0 et s_0, c'est-à-dire que le transducteur n'est pas inversible avec un retard de 0. En fait, il suffit de remarquer que A_0 n'a pas rang complet.

Comme le transducteur n'est pas inversible avec un délai de 0, il faut appliquer une transformation $G_{(4,0)}$. Ensuite, la première étape consiste à appliquer au système une séquence d'opérations élémentaires sur les lignes pour obtenir un système équivalent sous forme réduite, c'est-à-dire appliquer une transformation R_a . Ceci peut être obtenu en ajoutant la première et la deuxième ligne à la troisième :

$$\begin{bmatrix}1&0&0\\0&1&0\\1&1&1\end{bmatrix} y_t = \begin{bmatrix}1&1&0\\0&1&0\\0&0&0\end{bmatrix} x_{t+4} + \begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix} x_{t+3} + \begin{bmatrix}1&0&0\\0&1&0\\0&1&1\end{bmatrix} x_{t+2} + \begin{bmatrix}1&0&1\\0&1&1\\0&1&0\end{bmatrix} x_{t+1} \cdot x_t .$$

Il existe une équation qui ne dépend pas de x_{t+4} et peut donc être rejetée pour la le but d'obtenir x_4 à partir de s_0 et y_0y_1. L'étape suivante consiste à appliquer une transformation R_b , c'est-à-dire, de rejeter les équations qui ne dépendent pas de x_{t+4} et de réorganiser les autres en mettant ensemble les équations qui dépendent de x_{t+4} et qui ne dépendent pas des entrées suivantes. que, pour deux équations matricielles consécutives dans le système, réaffecter les lignes en mettant ensemble les deux premières lignes de la première équation et la dernière ligne de la deuxième équation. le résultat de cette procédure est le système suivant :

$$\begin{bmatrix}0&0&0\\0&0&0\\1&1&1\end{bmatrix} y_{t+1} + \begin{bmatrix}1&0&0\\0&1&0\\0&0&0\end{bmatrix} y_t = \begin{bmatrix}1&1&0\\0&1&0\\0&0&1\end{bmatrix} x_{t+4} + \begin{bmatrix}1&0&0\\0&1&0\\0&1&1\end{bmatrix} x_{t+3} + \begin{bmatrix}1&0&0\\0&1&0\\0&0&0\end{bmatrix} x_{t+2} + \begin{bmatrix}0&0&0\\0&0&0\\0&1&0\end{bmatrix} x_{t+2} \cdot x_{t+1} + \begin{bmatrix}1&0&1\\0&1&1\\0&0&0\end{bmatrix} x_{t+1} \cdot x_t , \quad \text{pour } t \geq 0.$$

La matrice des coefficients de x_{t+4} est inversible (a un rang complet), donc, en utilisant ce nouveau système, x_4 est déterminé de manière unique par s_0, y_0 et y_1, c'est-à-dire que le transducteur est inversible avec un retard de 1.

Pour construire un transducteur inverse d'un transducteur fini quasi-linéaire, comme dans le cas linéaire, on il suffit de multiplier, à gauche, l'équation du système résultant de rang complet par l'inverse de la matrice des coefficients de x_h.

Exemple 4.3.2. Soit M le transducteur fini quasi-linéaire présenté dans l'exemple précédent. Considérez le système qui a un rang complet qui définit le transducteur.

$$\begin{bmatrix}1&1&0\\0&1&0\\0&0&1\end{bmatrix} \begin{bmatrix}1&1&0\\0&1&0\\0&0&1\end{bmatrix} = \begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix} ,$$

on peut obtenir un transducteur inverse en multipliant le système de rang complet par $L = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$:

$$\begin{bmatrix} 0&0&0\\0&0&0\\1&1&1 \end{bmatrix} y_{t+1} + \begin{bmatrix} 1&1&0\\0&1&0\\0&0&0 \end{bmatrix} y_t = \begin{bmatrix} 1&0&0\\0&1&0\\0&0&1 \end{bmatrix} x_{t+4} + \begin{bmatrix} 1&1&0\\0&1&0\\0&1&1 \end{bmatrix} x_{t+3} + \begin{bmatrix} 1&1&0\\0&1&0\\0&0&0 \end{bmatrix} x_{t+2}$$

$$+ \begin{bmatrix} 0&0&0\\0&0&0\\0&1&0 \end{bmatrix} x_{t+2} \cdot x_{t+1} + \begin{bmatrix} 1&1&1\\0&1&1\\0&1&0 \end{bmatrix} x_{t+1} \cdot x_t \ , \ \text{pour } t \geq 0.$$

Alors, le transducteur inverse de M est le transducteur $M = F_2^3, F_2^3, F_2^{15}, \delta$, λ avec mémoire de ordre (1, 4) défini par le système infini :

$$x_{t+4} = \begin{bmatrix} 0&0&0\\0&0&0\\1&1&1 \end{bmatrix} y_{t+1} + \begin{bmatrix} 1&1&0\\0&1&0\\0&0&0 \end{bmatrix} y_t + \begin{bmatrix} 1&1&0\\0&1&0\\0&1&1 \end{bmatrix} x_{t+3} + \begin{bmatrix} 1&1&0\\0&1&0\\0&0&0 \end{bmatrix} x_{t+2} +$$

$$+ \begin{bmatrix} 0&0&0\\0&0&0\\0&1&0 \end{bmatrix} x_{t+2} \cdot x_{t+1} + \begin{bmatrix} 1&1&0\\0&1&1\\0&0&0 \end{bmatrix} x_{t+1} \cdot x_t \ , \ \text{pour } t \geq 0.$$

Comme Renji Tao l'a défini, les transducteurs finis quasi-linéaires τ avec mémoire d'ordre (h, k), où τ N et h, k N0, le critère d'inversibilité du transducteur fini linéaire avec mémoire peut être appliqué pour eux, c'est-à-dire qu'un τ-QLFT avec mémoire est inversible avec un délai r N0, $r \leq \tau$, si et seulement si, après en appliquant les transformations r $G(h,k)$, le système qui définit le transducteur a le rang complet. les transducteurs finis linéaires ont été définis de cette façon, dans la mesure où nous en déduisons, car, après un maximum de Transformations τ $G(h,k)$, le symbole d'entrée x_h n'apparaît que dans la partie linéaire du transducteur.

Pour les transducteurs finis quasi-linéaires définis de manière générale, comme dans la section 3.4.2, nous aurons un critère différent. Soit M = X , Y, $X^h \times Y^k$, δ, λ soit un transducteur fini quasi-linéaire avec mémoire d'ordre (h, k), h, k N0. Pour commencer, M peut être inversible avec un retard τ N0, pour vérifier τ = 0, 1, h dim(X), comme transducteurs finis linéaires avec mémoire, puisque la procédure pour l'inversibilité est la même. Cependant, pour pouvoir récupérer x_h après les transformations τ $G(h,k)$, dans en plus de la matrice des coefficients de x_h devant être inversible, x_h ne peut apparaître que dans le linéaire partie. Cette nouvelle exigence est facile à comprendre. Supposons que, dans le système infini qui définit le transducteur M après τ G(h,k) transformations, on a x_h dans la partie non linéaire du transducteur, par exemple $x_h \cdot x_{h-1}$. L'opération · n'est pas réversible, car connaître x_{h-1} ne ne nous permet pas de récupérer x_h. Par conséquent, x_h ne peut pas apparaître dans la partie non linéaire du transducteur.

Exemple 4.3.3. Soit $M = \langle \mathbb{F}_2^3, \mathbb{F}_2^3, \mathbb{F}_2^6, \delta, \lambda \rangle$ être un transducteur fini quasi-linéaire avec mémoire d'entrée d'ordre 2 défini par :

$$\begin{aligned} y_t &= A_0x_{t+2} + A_1x_{t+1} + A_2x_t + f(x_t , x_{t+1}) \\ &= \begin{bmatrix} 1&0&0\\0&1&0\\0&0&0 \end{bmatrix} x_{t+2} + \begin{bmatrix} 0&0&1\\1&0&1\\0&0&0 \end{bmatrix} x_{t+1} + \begin{bmatrix} 0&1&0\\0&0&1\\0&1&1 \end{bmatrix} x_t + \begin{bmatrix} 1&1&1\\1&1&0\\0&0&0 \end{bmatrix} x_{t+1} \cdot x_t , \quad \text{pour } t \geq 0, \end{aligned}$$

où $(x_t)_{t\geq0} \subseteq \mathbb{F}_2^3$ et $s_0 = \langle x_0, x_1 \rangle \in \mathbb{F}_2^6$ est l'état initial du transducteur. Soit $(x_t)_{t\geq2}$ être une séquence d'entrée et considérer $(y_t)_{t\geq0} = \lambda(s_0,(x_t)_{t\geq2})$.

Notez que la troisième colonne de A_0 est nulle. Par conséquent, y_0 ne contient aucune information sur la troisième composante de x_2. Par conséquent, le transducteur n'est pas inversible avec un retard de 0.

Comme le transducteur n'est pas inversible avec un retard de 0, il faut appliquer une transformation G(2,0) . système est sous forme réduite, il n'est donc pas nécessaire d'appliquer une transformation Ra . Il y en a une équation qui ne dépend pas de x_{t+2}, il faut donc appliquer une transformation Rb à la système infini :

$$\begin{cases} \vdots \\ y_t = \begin{bmatrix} 1&0&0\\0&1&0\\0&0&0 \end{bmatrix} x_{t+2} + \begin{bmatrix} 0&0&1\\1&0&1\\0&0&0 \end{bmatrix} x_{t+1} + \begin{bmatrix} 0&1&0\\0&0&1\\0&1&1 \end{bmatrix} x_t + \begin{bmatrix} 1&1&1\\1&1&0\\0&0&0 \end{bmatrix} x_{t+1} \cdot x_t \\ y_{t+1} = \begin{bmatrix} 1&0&0\\0&1&0\\0&0&0 \end{bmatrix} x_{t+3} + \begin{bmatrix} 0&0&1\\1&0&1\\0&0&0 \end{bmatrix} x_{t+2} + \begin{bmatrix} 0&1&0\\0&0&1\\0&1&1 \end{bmatrix} x_{t+1} + \begin{bmatrix} 1&1&1\\1&1&0\\0&0&0 \end{bmatrix} x_{t+2} \cdot x_{t+1} \\ \vdots \end{cases}.$$

Pour appliquer une transformation Rb , pour deux équations matricielles consécutives dans le système, réaffecter les lignes en rassemblant les deux premières lignes de la première équation et la dernière ligne de la deuxième équation. Le résultat de cette procédure est le système suivant :

$$\begin{bmatrix}0&0&0\\0&0&0\\0&0&1\end{bmatrix} y_{t+1} + \begin{bmatrix}1&0&0\\0&1&0\\0&0&0\end{bmatrix} y_t = \begin{bmatrix}1&0&0\\0&1&0\\0&0&0\end{bmatrix} x_{t+2} + \begin{bmatrix}0&0&1\\1&0&1\\0&1&1\end{bmatrix} x_{t+1} + \begin{bmatrix}0&1&0\\0&0&1\\0&0&0\end{bmatrix} x_t + \begin{bmatrix}1&1&1\\1&1&0\\0&0&0\end{bmatrix} x_{t+1} \cdot x_t \quad , \text{ pour } t \geq 0.$$

La matrice A0 n'a pas de rang complet donc le transducteur n'est pas inversible avec un retard de 1.

il est nécessaire d'appliquer une autre transformation G(2,0) . Comme le système est sous forme réduite, une seule il faut appliquer une transformation Rb . On obtient ainsi :

$$\begin{bmatrix}0&0&0\\0&0&0\\0&0&1\end{bmatrix} y_{t+2} + \begin{bmatrix}1&0&0\\0&1&0\\0&0&0\end{bmatrix} y_t = \begin{bmatrix}1&0&0\\0&1&0\\0&1&1\end{bmatrix} x_{t+2} + \begin{bmatrix}0&0&1\\1&0&1\\0&0&0\end{bmatrix} x_{t+1} + \begin{bmatrix}0&1&0\\0&0&1\\0&0&0\end{bmatrix} x_t + \begin{bmatrix}1&1&1\\1&1&0\\0&0&0\end{bmatrix} x_{t+1} \cdot x_t \quad , \text{ pour } t \geq 0.$$

Maintenant le système a un rang complet, donc le transducteur M est inversible avec un délai de 2.

Exemple 4.3.4. Soit M = F_2^3, F_2^3, F_2^9, δ, λ être un transducteur fini quasi-linéaire avec mémoire d'entrée d'ordre 3 défini par :

$$y_t = A_0x_{t+3} + A_1x_{t+2} + A_2x_{t+1} + A_3x_t + f(x_t, x_{t+1}, x_{t+2})$$

$$= \begin{bmatrix}1&0&0\\0&1&0\\0&0&0\end{bmatrix} x_{t+3} + \begin{bmatrix}0&1&1\\0&0&1\\0&0&0\end{bmatrix} x_{t+2} + \begin{bmatrix}1&0&1\\1&1&1\\0&0&0\end{bmatrix} x_{t+1} + \begin{bmatrix}0&1&0\\1&0&1\\0&1&0\end{bmatrix} x_t + \begin{bmatrix}0&1&1\\1&1&0\\0&0&0\end{bmatrix} x_{t+1} \cdot x_t,$$

pour $t \geq 0$, où $(x_t)_{t\geq 0}$ F_2^3 et $s_0 =< x_0, x_1, x_2 >$ F_2^3 est l'état initial du transducteur. Soit $(x_t)_{t\geq 3}$ une séquence d'entrée et considérons $(y_t)_{t\geq 0} = \lambda(s_0,(x_t)_{t\geq 3})$.

Comme A0 n'a pas de rang complet, le transducteur n'est pas inversible avec un retard de 0. Par conséquent, un doit appliquer une transformation G(3,0) . Le système est sous forme réduite, il suffit donc de appliquer une transformation Rb . Le système résultant est :

$$\begin{bmatrix}0&0&0\\0&0&0\\0&0&1\end{bmatrix} y_{t+1} + \begin{bmatrix}1&0&0\\0&1&0\\0&0&0\end{bmatrix} y_t = \begin{bmatrix}1&0&0\\0&1&0\\0&0&0\end{bmatrix} x_{t+3} + \begin{bmatrix}0&1&1\\0&0&1\\0&0&0\end{bmatrix} x_{t+2} + \begin{bmatrix}1&0&1\\1&1&1\\0&1&0\end{bmatrix} x_{t+1} + \begin{bmatrix}0&1&0\\1&0&1\\0&0&0\end{bmatrix} x_t + \begin{bmatrix}0&1&1\\1&1&0\\0&0&0\end{bmatrix} x_{t+1} \cdot x_t, \text{ pour } t \geq 0.$$

Notez que l'ajout de la connaissance de y_{t+1} ne donne aucune information sur le troisième composant de x_{t+3}, puisque le rang du système est le même qu'avant. La même chose se produira avec y_{t+2}. Après 3 transformations $G(3,0)$ on obtient le système suivant :

$$\begin{bmatrix}0&0&0\\0&0&0\\0&0&1\end{bmatrix} y_{t+3} + \begin{bmatrix}1&0&0\\0&1&0\\0&0&0\end{bmatrix} y_t = \begin{bmatrix}1&0&0\\0&1&0\\0&1&0\end{bmatrix} x_{t+3} + \begin{bmatrix}0&1&1\\0&0&1\\0&0&0\end{bmatrix} x_{t+2} + \begin{bmatrix}1&0&1\\1&1&1\\0&0&0\end{bmatrix} x_{t+1} + \begin{bmatrix}0&1&0\\1&0&1\\0&0&0\end{bmatrix} x_t + \begin{bmatrix}0&1&1\\1&1&0\\0&0&0\end{bmatrix} x_{t+1} \cdot x_t, \text{ pour } t \geq 0.$$

Enfin, il faut appliquer une transformation $G(3,0)$ supplémentaire . Le système résultant de l'application d'une transformation Ra transformation et une transformation Rb est donnée par :

$$\begin{bmatrix}0&0&0\\0&0&0\\0&0&1\end{bmatrix} y_{t+4} + \begin{bmatrix}0&0&0\\0&0&0\\0&1&0\end{bmatrix} y_{t+1} + \begin{bmatrix}1&0&0\\0&1&0\\0&0&0\end{bmatrix} y_t = \begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix} x_{t+3} + \begin{bmatrix}0&1&1\\0&0&1\\1&1&1\end{bmatrix} x_{t+2} + \begin{bmatrix}1&0&1\\1&1&1\\1&0&1\end{bmatrix} x_{t+1} + \begin{bmatrix}0&1&0\\1&0&1\\0&0&0\end{bmatrix} x_t + \begin{bmatrix}0&0&0\\0&0&0\\1&1&0\end{bmatrix} x_{t+2} \cdot x_{t+1} + \begin{bmatrix}0&1&1\\1&1&0\\0&0&0\end{bmatrix} x_{t+1} \cdot x_t, \text{ pour } t \geq 0.$$

Le système résultant a un rang complet, donc le transducteur M est inversible avec un retard de 4. que le retard est supérieur à l'ordre de la mémoire.

Chapitre 5

L'attaque de Bao-Igarashi contre FAPCK

5.1 Composition des transducteurs finis

La composition des transducteurs finis est une opération essentielle sur les systèmes cryptographiques en cours de discussion. La sécurité de ces cryptosystèmes est, en un sens, basée sur le problème de factorisation des transducteurs finis non linéaires. Renji Tao a présenté, dans son livre [Tao09], deux compositions de transducteurs finis. Dans cette section, on présentera ces compositions, qui on appelle composition habituelle et composition spéciale.

Définition 5.1.1. Soit $M_i = X_i, Oui, S_i, \delta_i, \lambda_i$, $i = 1, 2$, soient deux transducteurs finis avec $Y_1 = X_2$. La composition habituelle de M_1 et M_2, notée $M_2 \circ M_1$, est le transducteur

$$M_2 \circ M_1 = X_1, Y_2, S_1 \times S_2, \delta, \lambda$$

où, pour x X_1, s_1 S_1 et s_2 S_2,

$$\delta((s_1, s_2), x) = (\delta(s_1, x), \delta(s_2, \lambda(s_1, x)))$$

$$\lambda((s_1, s_2), x) = \lambda_2(s_2, \lambda_1(s_1, x)).$$

Fondamentalement, dans la composition habituelle, la sortie du premier transducteur M1 est l'entrée du deuxième transducteur M2.

Pour introduire la composition spéciale, rappelons l'application de remplacement définie dans la section 3.3 : soit X être un ensemble non vide et j N, l'application de remplacement est définie par

$$\sigma : X^j \times X \longrightarrow X^j$$

$$((x_1, x_2, \ldots, x_j), x) \longrightarrow (x_2, \ldots, x_j, x).$$

De plus, étant donné un ensemble X, n N, et i, j N tels que i+j ≤ n+ 1, définissons la (i, j)-projection carte:

$$\pi_{i,j} : X^n \longrightarrow X^j$$

$$(x_1, x_2, \ldots, x_n) \longrightarrow (x_i, x_{i+1}, \ldots, x_{i+j-1}).$$

Pour toute application $h : X^{n+1} \longrightarrow Y$ (n N_0), et pour tout m N, on notera h^{+m} l'application $h^{+m} : X^{n+m} \longrightarrow Y^m$ donnée par $h^{+m}(x) = (h \circ \pi_{1,n+1}(x), h \circ \pi_{2,n+1}(x), \ldots, h \circ \pi_{m,n+1}(x))$, pour tout x X^{n+m}.

Définition 5.1.2. Soient M_f et M_g deux transducteurs finis à mémoire induite par les fonctions

$$f : X^{h_f} \times X \longrightarrow Y \text{ et } g : Y^{h_g} \times Z^k \times Y \longrightarrow Z,$$

c'est-à-dire que M_f est un transducteur avec une mémoire d'entrée d'ordre h_f et M_g est un transducteur avec une mémoire d'ordre (h_g, k). La composition spéciale de M_f et M_g, notée $M_g \bullet M_f$, est le transducteur avec mémoire d'ordre $(h_f + h_g, k)$

$$M_g \bullet M_f = X, \delta, \lambda, Z, X^{h_f + h_g} \times Z^k ,$$

où δ et λ sont donnés, pour x $X^{h_f + h_g}$, z Z^k, et a X, par

$$\delta((x, z), a) = (\sigma(x, a), \sigma(z, \quad (x, z, a))),$$

$$\lambda((x, z), a) = \quad (x, z, a),$$

où $(x, z, a) = g(f \circ \pi_{1,h_f+1}(x), f \circ \pi_{2,h_f+1}(x), \ldots, f \circ \pi_{h_g,h_f+1}(x), z, f \circ \sigma(\pi_{h_g,h_f+1}(x), a)) = g(f^{+h_g}(x), z, f \circ \sigma(\pi_{h_g,h_f+1}(x), a))$ Z.

On peut maintenant se demander quelle est la relation entre $M_g \circ M_f$ et $M_g \bullet M_f$. Renji Tao a montré la résultat suivant [Tao09, Théorème 1.2.1].

5.1.3. Soit $M_f = X, \delta_g, \lambda_g$ comme , Y, X^{h_f}, δ_f, λ_f et $M_g = Y, Z, Y^{h_g} \times Z^k$ Proposition ci-dessus. Ensuite, pour chaque état dans $M_g \bullet M_f$ il existe un état équivalent dans $M_g \circ M_f$.

Preuve. Soit $s = (x, z)$ $X^{hf+hg} \times Z^k$ un état de $M_g \bullet M_f$, et définir

$$s_f = \pi_{hg+1,hf}(x), \quad s_g = (f^{+hg}(x), z).$$

Nous allons montrer que l'état (s_f, s_g) $X^{hf} \times Y^{hg} \times Z^k$ de $M_g \circ M_f$ est équivalent à l'état s.

Notez que $(s_f, a) = \sigma(\pi_{hg,hf+1}(x), a)$, et donc

$$\lambda_\circ((s_f, s_g), a) = \lambda_g(s_g, \lambda_f(s_f, a)) = \lambda_g(s_g, f(s_f, a)) = \lambda_g(s_g, f \circ \sigma(\pi_{hg,hf+1}(x), a))$$
$$= \lambda_g(f^{+hg}(x), z, f \circ \sigma(\pi_{hg,hf+1}(x), a))$$
$$= g(f^{+hg}(x), z, f \circ \sigma(\pi_{hg,hf+1}(x), a))$$
$$= \lambda_\bullet((x, z), a) = \lambda_\bullet(s, a).$$

Aussi,

$$\delta_\circ((s_f, s_g), a) = (\delta_f(s_f, a), \delta_g(s_g, \lambda_f(s_f, a)))$$
$$= (\delta_f(s_f, a), \delta_g((f^{+hg}(x), z), f(s_f, a))) =$$
$$(\sigma(s_f, a), \sigma(f^{+hg}(x), f(s_f, a)), \sigma(z, g(f^{+hg}(x), z, f(s_f, a)))),$$

alors que

$$\tilde{s} = \lambda_\bullet(s, a) = \lambda_\bullet((x, z), a)$$
$$= (\sigma(x, a), \sigma(z, g(f^{+hg}(x), z, f \circ \sigma(\pi_{hg,hf+1}(x), a)))) =$$
$$(\sigma(x, a), \sigma(z, g(f^{+hg}(x), z, f(s_f, a))))$$
$$=: (\tilde{x}, \tilde{z}).$$

Maintenant, notez que

$$(\tilde{s}_f = \pi_{hg+1,hf}(\tilde{x}) = \pi_{hg+1,hf}(\sigma(x, a)) = \sigma(\pi_{hg+1,hf}(x), a) = \sigma(s_f, a), \tilde{s}_g$$
$$= (f^{+hg}(\tilde{x}), \tilde{z}) = (f^{+hg}(\sigma(x, a)), \sigma(z, g(f^{+hg}(x), z, f(s_f, a)))).$$

Ainsi, pour montrer que $\delta_\circ((s_f, s_g), a) = (\tilde{s}_f, \tilde{s}_g)$, il suffit de vérifier que $f^{+hg}(\sigma(x, a)) = \sigma(f^{+hg}(x), f(s_f, a))$:

$$\sigma(f^{+hg}(x), f(s_f, a)) = \sigma(f^{+hg}(x), f(\pi_{hg+1,hf}(x), a))$$
$$= \sigma(f \circ \pi_{1,hf+1}(x), f \circ \pi_{2,hf+1}(x), \ldots, f \circ \pi_{hg,hf+1}(x), f(\pi_{hg+1,hf}(x), a))$$
$$= (f \circ \pi_{2,hf+1}(x), \ldots, f \circ (\pi_{hg,hf+1}(x), a)) = f^{+hg}(\sigma(x, a)).$$

□

Notez que, étant donné une séquence d'entrée α X hf + hg et deux états équivalents, s X hf + hg × Zk de Mg • Mf et (sf , sg) X hf × Yhg × Zk de Mg ◦ Mf , comme défini ci-dessus, tous deux composés les transducteurs produisent la même sortie. Étant donné que pour chaque état dans Mg • Mf, il existe un équivalent état dans Mg ◦ Mf , on peut utiliser la composition habituelle au lieu de la composition spéciale, si l'on choisit un état initial de Mg ◦ Mf qui est équivalent à un état dans Mg • Mf .

Dans le FAPKC, les transducteurs à clé publique sont obtenus à l'aide de la composition spéciale. De plus, puisque chaque état possède un état équivalent dans le transducteur obtenu avec la composition habituelle, dans le FAPKC, on n'utilise jamais un état initial qui n'est pas équivalent à celui de la clé publique transducteur. Par conséquent, pour l'instant, on utilisera indifféremment le transducteur habituel et le transducteur spécial composition en référence au transducteur à clé publique.

Mf = X , δg, λg deux transducteurs Y, X hf, δf, λf et Mg = Y, Z, Y hg × Zk Soient

Pour calculer l'équation qui définit le transducteur composé M, on peut utiliser l'une des compositions présentées, puisque leur rendement est le même. Si l'on connaît Mf et Mg, le composé le transducteur sera considéré comme Mg ◦ Mf , car la composition habituelle est plus naturelle. Cependant, quand on ne connaît que M, il faut le voir comme Mg •Mf , car les symboles dans Y n'ont pas de sens. Dans le cas de la connaissance de Mf et Mg, si l'on ne connaît que l'état initial s X hf +hg × Zk de M, alors il faut trouver l'état équivalent (sf , sg) X hf × Yhg × Zk pour pouvoir utiliser l'habituel composition.

Exemple 5.1.4. Soit Mf = $\mathbb{F}_2^3, \mathbb{F}_2^3, \mathbb{F}_2^6$, δf , λf soient un transducteur fini linéaire avec mémoire d'entrée d'ordre 2 et Mg = $\mathbb{F}_2^3, \mathbb{F}_2^3, \mathbb{F}_2^{12}$, δg, λg soit un transducteur fini linéaire avec mémoire d'ordre (1, 3). Mf et Mg sont définis comme suit :

$$M_f : y_t = \begin{bmatrix} 1&0&0\\ 0&1&0\\ 0&0&0 \end{bmatrix} x_{t+2} + \begin{bmatrix} 1&0&0\\ 0&1&1\\ 0&0&1 \end{bmatrix} x_{t+1} + \begin{bmatrix} 1&0&1\\ 0&0&0\\ 0&1&0 \end{bmatrix} x_t, \quad \text{pour } t \geq 0.$$

$$M_g : z_{t+3} = \begin{bmatrix} 1&1&0\\ 0&1&0\\ 0&0&1 \end{bmatrix} y_{t+1} + \begin{bmatrix} 1&1&0\\ 0&0&0\\ 1&0&0 \end{bmatrix} y_t + \begin{bmatrix} 1&0&1\\ 0&0&1\\ 0&0&0 \end{bmatrix} z_{t+2} + \begin{bmatrix} 1&0&0\\ 0&1&0\\ 0&1&0 \end{bmatrix} z_t, \quad \text{pour } t \geq 0.$$

Pour calculer le transducteur composé M = Mg ◦ Mf , il suffit de substituer le $(y_t)_{t\geq 0}$ symboles dans l'équation de Mg par les relations de $(x_t)_{t\geq 0}$, obtenues avec l'équation de Mf .

Depuis

$$\begin{pmatrix} 1&1&0\\0&1&0\\0&0&1 \end{pmatrix} y_{t+1} = \begin{pmatrix} 1&1&0\\0&1&0\\0&0&0 \end{pmatrix} x_{t+3} + \begin{pmatrix} 1&1&1\\0&1&1\\0&0&1 \end{pmatrix} x_{t+2} + \begin{pmatrix} 1&0&1\\0&0&0\\0&1&0 \end{pmatrix} x_{t+1}, \text{ pour } t \geq 0. \text{ et}$$

$$\begin{pmatrix} 1&1&0\\0&0&0\\1&0&0 \end{pmatrix} y_{t} = \begin{pmatrix} 1&1&0\\0&0&0\\1&0&0 \end{pmatrix} x_{t+2} + \begin{pmatrix} 1&1&1\\0&0&0\\1&0&0 \end{pmatrix} x_{t+1} + \begin{pmatrix} 1&0&1\\0&0&0\\1&0&1 \end{pmatrix} x_{t}, \quad \text{pour } t \geq 0,$$

le transducteur composé M a une mémoire d'ordre (2 + 1, 3) = (3, 3) et est donné par :

$$M : z_{t+3} = \begin{pmatrix} 1&1&0\\0&1&0\\0&0&0 \end{pmatrix} x_{t+3} + \begin{pmatrix} 0&0&1\\0&1&1\\1&0&1 \end{pmatrix} x_{t+2} + \begin{pmatrix} 0&1&0\\0&0&0\\1&1&0 \end{pmatrix} x_{t+1} + \begin{pmatrix} 1&0&1\\0&0&0\\1&0&1 \end{pmatrix} x_{t}$$

$$+ \begin{pmatrix} 1&0&1\\0&0&1\\0&0&0 \end{pmatrix} z_{t+2} + \begin{pmatrix} 1&0&0\\0&1&0\\0&1&0 \end{pmatrix} z_{t}, \quad \text{pour } t \geq 0.$$

Théorème 5.1.5. Soient $M_0 = X , Y, S_0, \delta_0, \lambda_0$ et $M_1 = Y, Z, S_1, \delta_1, \lambda_1$ deux trans-
injectifs avec retard τ_0 N_0 et τ_1 N_0, respectivement. Le transducteur composé $M = M_1 \circ M_0 = X , Z, S, \delta, \lambda$ est injectif avec un délai $\tau_0 + \tau_1$.

Preuve. Le transducteur M est injectif avec un retard $\tau_0 + \tau_1$ si

$$S, \quad x, x \quad X \quad , \quad \mu, \mu \quad X^{\tau_0+\tau_1} , \lambda(s, x\mu) = \lambda(s, x\mu) = \quad x = x . \quad s$$

Comme les transducteurs M_0 et M_1 sont injectifs avec un retard τ_0 et τ_1 respectivement, on a :

$$S_0, \quad x, x \quad X , \quad \alpha, \alpha \quad X^{\tau_0} \quad , \lambda_0(s_0, x\alpha) = \lambda_0(s_0, x\alpha) = \quad x = x \quad s_0 \quad ,$$

$$s_1 \quad S_1, \quad y, y \quad Y, \quad \beta, \beta \quad Y^{\tau_1} , \lambda_1(s_1, y\beta) = \lambda_1(s_1, y\beta) = \quad y = y .$$

Soit x, x X , α_{τ_0} , α_{τ_0} X^{τ_0} , α_{τ_1} , α_{τ_1} X^{τ_1}, $\mu = \alpha_{\tau_0}\alpha_{\tau_1}$ $X^{\tau_0+\tau_1}$ et $\mu = \alpha$ $_{\alpha_{\tau_0}\tau_1}$ $X^{\tau_0+\tau_1}$.

Soit s_0 S_0, s_1 S_1 et $s = (s_0, s_1)$ S. Rappelons la définition de la fonction de sortie dans la composition habituelle présentée dans la définition 5.1.1 : $\lambda((s_0, s_1), x) = \lambda_1(s_1, \lambda_0(s_0, x))$. Ensuite, la les énoncés suivants sont équivalents :

$$\lambda(s, x\mu) = \lambda(s, x\mu)$$

$$\lambda_1(s_1, \lambda_0(s_0, x\mu)) = \lambda_1(s_1, \lambda_0(s_0, x\mu))$$

$$\lambda_1(s_1, \lambda_0(s_0, x\alpha_{\tau_0}\alpha_{\tau_1})) = \lambda_1(s_1, \lambda_0(s_0, x\alpha \quad _{\alpha_{\tau_0}\tau_1})).$$

Machine Translated by Google

Soit $\lambda_0(s_0, x\alpha_{\tau 0}\alpha_{\tau 1}) = y\beta_{\tau 0}\beta_{\tau 1}$ et $\lambda_0(s_0, x\alpha_{\alpha\tau 0\tau 1}) = y\beta_{\tau 0}\beta_{\tau 1}$, pour certains y, y Y, $\beta_{\tau 0}$, $\beta_{\tau 0}$ $Y_{\tau 0}$ et $\beta_{\tau 1}$, $\beta_{\tau 1}$ $Y_{\tau 1}$. M1 est injectif de retard τ1, alors y = y et $\beta_{\tau 0} = \beta_{\tau 0}$ Il s'ensuit que

$$y\beta_{\tau 0} = y\beta_{\tau 0} \quad \lambda_0(s_0, x\alpha_{\tau 0}) = \lambda_0(s_0, x\alpha_{\tau 0}).$$

Puisque M0 est injectif avec un retard τ0, on a x = x . On peut en conclure que M est injectif avec retard τ0 + τ1. □

Notez que, dans la preuve précédente, la formule de la fonction de sortie a été utilisée de la manière habituelle. composition. Cependant, il a été prouvé dans la proposition 5.1.3 que la sortie du composé le transducteur est le même dans la composition habituelle et dans la composition spéciale, par conséquent, le résultat est également valable pour la composition spéciale.

Exemple 5.1.6. Les transducteurs M0 et M1 présentés dans l'exemple 5.1.4 sont inversibles avec délai 1 et 0, respectivement. Le transducteur M = M1 ◦ M0 est inversible avec un délai de 1.

5.2 Description générale des FAPKC

Le premier système FAPKC a été proposé en 1985 par Tao et Chen dans un article (en chinois) et a été nommé FAPKC0. Une description en anglais en a été présentée dans un ouvrage ultérieur du même nom auteurs [TC86]. Dans ce système, la clé privée est composée des inverses de deux clés injectives transducteurs à mémoire, où l'un est un transducteur fini linéaire τ -injectif (τ > 15), et le l'autre est un transducteur fini quasi-linéaire avec un retard de 0. Cette inverse peut être facilement calculée, comme vu dans le dernier chapitre. La clé publique est le résultat de la composition de la paire d'origine, obtenant ainsi un transducteur fini non linéaire. En 1986, Tao et Chen ont publié deux variantes du cryptosystème FAPKC0, nommé FAPKC1 et FAPKC2 [TC86]. Dans FAPKC1, les deux les transducteurs finis dont les inverses composent la clé privée ont les mêmes caractéristiques que dans FAPKC0. Mais, dans FAPKC2, le transducteur quasi-linéaire est inversible avec un délai différent de celui zéro. Plus tard, deux nouveaux schémas cryptographiques sont apparus : FAPKC3 et FAPKC4, présentés par Tao et al. [TCC97] et par Tao et Chen [TC97], respectivement. Entre-temps, d'autres schémas de La cryptographie à clé publique basée sur des transducteurs finis a été développée (le système FAPKC93 a été présenté dans une thèse de doctorat rédigée en chinois, et une variante de FAPKC2 a été proposée par Bao et Igarashi [BI95]). Tous ces systèmes ont une structure similaire, leur principale différence étant la choix des transducteurs pour la clé privée.

Le point crucial de la sécurité de ces cryptosystèmes est qu'il est facile d'obtenir un inverse de la transducteur composé à partir des inverses de ses facteurs, alors qu'il est considéré comme difficile de trouver que inverse sans connaître ces facteurs. D'autre part, la factorisation d'un transducteur Cela semble être difficile en soi.

On sait que, si l'un des transducteurs finis à l'origine de la clé privée est linéaire et que l'autre est inversible avec un délai de 0, le cryptosystème n'est pas sécurisé [BI95] (ce qui est le cas de FAPKC0, FAPKC1 et FAPKC93). Cependant, si les deux transducteurs finis sont quasi-linéaires ou l'un d'eux est linéaire et le délai de l'autre est supérieur à 0, les FAPKC semblent sécurisés chaque fois qu'un soi-disant Le processus de vérification linéaire Ra Rb est inclus dans le générateur de clés [Tao95]. FAPKC2, FAPKC3 et FAPKC4 sont des exemples de tels FAPKC.

Dans la section suivante, nous allons présenter l'attaque Bao-Igarashi contre FAPKC. Afin de comprendre l'attaque, tout d'abord, présentons correctement ces cryptosystèmes.

5.2.1 Systèmes cryptographiques FAPKC

Dans tous les FAPKC, la clé privée est composée des inverses de deux ou plusieurs transducteurs finis et leurs états initiaux. La clé publique est donnée par la composition de tous les transducteurs finis dont les inverses sont dans la clé privée, ainsi que son état initial. Habituellement, l'entrée et la sortie sont des vecteurs à 8 dimensions sur F_2, puisque tous les caractères peuvent être représentés par un octet. la différence entre ces cryptosystèmes est le type de transducteurs qui génèrent le privé clé. Le FAPKC tel que présenté dans cette section est la base de tous les FAPKC. Bien qu'il ait été prouvé comme non sûr (l'attaque sera présentée dans la section suivante), ce schéma est l'un des rares pour lesquels il est possible de construire des exemples. Pour les versions indiquées comme plus sûres, il n'y a pas exemples disponibles et la méthode présentée par l'auteur n'est pas claire.

La procédure de génération de paires de clés est la suivante :

1. Choisissez un transducteur fini quasi-linéaire à mémoire, M_0, inversible avec un délai de 0. Calculez un transducteur inverse de M_0, M_0^{-1} ;

2. Choisir un transducteur fini linéaire à mémoire, M_1, inversible avec un retard τ (typiquement τ > 15). Calculer un transducteur inverse de M_1, noté M_1^{-1} ;

3. Calculez le transducteur composé M à partir de M0 et M1, et choisissez l'état initial sM ;

4. La clé privée est la paire (M_0^{-1}, M_1^{-1}). La clé publique est le transducteur composé et son état initial, c'est-à-dire (M, sM).

Dans FAPKC, un texte en clair est chiffré à l'aide du transducteur à clé publique M, un transducteur fini non linéaire. transducteur avec retard τ . Le texte en clair est la séquence d'entrée de M, et la sortie est la texte chiffré. Notez que, puisque le transducteur est inversible avec un retard τ , il faut ajouter le texte en clair avec τ symboles choisis arbitrairement pour que le destinataire puisse récupérer le message complet.

Pour décrypter le texte chiffré, il suffit d'utiliser les transducteurs inverses M_0^{-1} et M_1^{-1} dans le clé privée avec les états initiaux obtenus à partir des états inverses de ceux qui composent la état équivalent de sM pour la composition habituelle. Autre moyen possible de décrypter le texte chiffré consiste à calculer le transducteur inverse de M à partir de M_0^{-1} et M_1^{-1}, $M^{-1} = M_1^{-1} \circ M_0^{-1}$, et son état initial (l'état inverse de sM).

Le principe de cryptage et de décryptage de FAPKC est illustré dans les figures suivantes, où le le texte en clair est une séquence de longueur m + 1. M0 est un transducteur quasi-linéaire avec une mémoire d'entrée de ordre h0 N0 et retard 0, M1 est un transducteur linéaire à mémoire d'ordre (h1, k), h1, k N0, et retard τ N, et M'_0 et M'_1 sont les inverses respectifs. De plus, M est le composé transducteur de M0 et M1, et M son inverse.

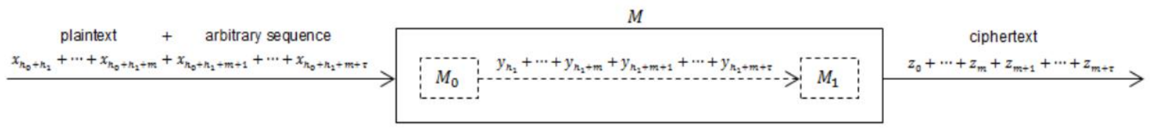


Figure 5.1 : Principe de cryptage de FAPKC

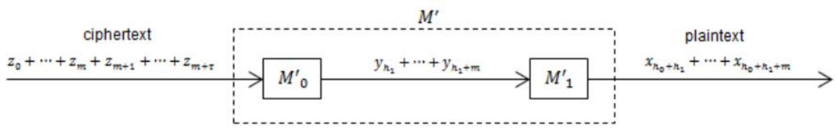


Figure 5.2 : Principe de décryptage de FAPKC

Ensuite, deux exemples simples des procédures de cryptage et de décryptage sur FAPKC seront présentés.

Soit M0 = $\langle \mathbb{F}_2^3, \mathbb{F}_2^3, \mathbb{F}_2^{36}, \delta_0, \lambda_0 \rangle$ et M1 = $\langle \mathbb{F}_2^3, \mathbb{F}_2^3, \mathbb{F}_2^{36}, \delta_1, \lambda_1 \rangle$ sont les transducteurs définis comme suit :

$$M0 : y_t = \begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix} x_{t+2} + \begin{bmatrix}1&0&0\\0&1&1\\0&0&0\end{bmatrix} x_{t+1} + \begin{bmatrix}1&0&1\\0&0&0\\0&1&0\end{bmatrix} x_t + \begin{bmatrix}0&0&0\\0&0&1\\1&0&0\end{bmatrix} x_{t+1}x_t , \quad \text{pour } t \geq 0.$$

$$M1 : z_t = \begin{bmatrix}1&0&0\\0&1&0\\0&0&0\end{bmatrix} y_{t+2} + \begin{bmatrix}1&0&1\\0&0&1\\0&0&0\end{bmatrix} y_{t+1} + \begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix} y_t , \quad \text{pour } t \geq 0.$$

M0 est un transducteur fini quasi-linéaire à mémoire d'entrée d'ordre 2 et inversible avec retard 0, et M1 est un transducteur linéaire avec mémoire d'entrée 2 et inversible avec retard 2. Pour calculer le transducteur composé $M = M1 \circ M0$, il suffit de substituer les symboles $(y_t)_{t \geq 0}$ dans le équation de M1 par les relations équivalentes de $(x_t)_{t \geq 0}$, obtenue avec l'équation de M0 :

$$\begin{aligned} M : z_t = {} & \begin{bmatrix}1&0&0\\0&1&0\\0&0&0\end{bmatrix} x_{t+4} + \begin{bmatrix}0&0&1\\0&1&0\\0&0&0\end{bmatrix} x_{t+3} + \begin{bmatrix}1&0&1\\0&1&0\\0&0&1\end{bmatrix} x_{t+2} + \begin{bmatrix}0&1&1\\0&0&1\\0&0&0\end{bmatrix} x_{t+1} + \begin{bmatrix}1&0&1\\0&0&0\\0&1&0\end{bmatrix} x_t \\ & + \begin{bmatrix}0&0&0\\0&0&1\\0&0&0\end{bmatrix} x_{t+3}x_{t+2} + \begin{bmatrix}1&0&0\\1&0&0\\0&0&0\end{bmatrix} x_{t+2}x_{t+1} + \begin{bmatrix}0&0&0\\0&0&1\\1&0&0\end{bmatrix} x_{t+1}x_t , \quad \text{pour } t \geq 0. \end{aligned}$$

Le transducteur composé est un transducteur fini non linéaire avec une mémoire d'entrée d'ordre 4 et inversible avec un délai de 2. Ensuite, la clé publique est composée du transducteur M et d'une valeur initiale état s, par exemple, $s = < x_0, x_1, x_2, x_3 > = < \begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}1\\1\\0\end{bmatrix}, \begin{bmatrix}0\\1\\1\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix} >$.

Exemple 5.2.1. Si l'on souhaite crypter un message au propriétaire de la clé publique présentée auparavant, il suffit de calculer la sortie en utilisant le transducteur M et l'état initial donné.

Par exemple, pour crypter $\alpha = x_4x_5 = \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}0\\0\end{pmatrix}$, on a :

$$z_0 = \lambda(< x_0, x_1, x_2, x_3 >, x_4) = \lambda\left(\left< \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix} \right>, \begin{pmatrix}1\\0\end{pmatrix}\right) = \begin{pmatrix}1\\0\end{pmatrix}.$$

$$z_1 = \lambda(< x_1, x_2, x_3, x_4 >, x_5) = \lambda\left(\left< \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix} \right>, \begin{pmatrix}0\\0\end{pmatrix}\right) = \begin{pmatrix}0\\0\end{pmatrix}.$$

Mais, comme le transducteur a un retard de 2, il faut ajouter au texte en clair 2 choisis arbitrairement symboles, disons $\beta = x_6x_7 = \begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}1\\1\end{pmatrix}$, et calculer le rendement respectif :

$$z_2 = \lambda(< x_2, x_3, x_4, x_5 >, x_6) = \lambda\left(\left< \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\0\end{pmatrix} \right>, \begin{pmatrix}0\\1\end{pmatrix}\right) = \begin{pmatrix}1\\1\end{pmatrix}.$$

$$z_3 = \lambda(< x_3, x_4, x_5, x_6 >, x_7) = \lambda\left(\left< \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix} \right>, \begin{pmatrix}1\\1\end{pmatrix}\right) = \begin{pmatrix}1\\0\end{pmatrix}.$$

Alors, le texte chiffré est $\lambda(s, \alpha\beta) = \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}0\\0\end{pmatrix}\begin{pmatrix}1\\1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}.$

Pour le processus de décryptage, il est nécessaire de calculer les inverses des transducteurs M_0 et M_1, qui sera la clé privée. Pour cela, il suffit d'appliquer la procédure présentée au chapitre 4. Ainsi, les transducteurs inverses sont définis par :

$$M_0^{-1}: x_{t+2} = \begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix} y_t + \begin{pmatrix}1&0&0\\0&1&1\\0&0&0\end{pmatrix} x_{t+1} + \begin{pmatrix}1&0&1\\0&0&0\\0&1&0\end{pmatrix} x_t + \begin{pmatrix}0&0&0\\0&0&1\\1&0&0\end{pmatrix} x_{t+1}x_t, \quad \text{pour } t \geq 0.$$

$$M_1^{-1}: y_{t+2} = \begin{pmatrix}0&0&0\\0&0&0\\0&0&1\end{pmatrix} z_{t+2} + \begin{pmatrix}1&0&0\\0&1&0\\0&0&0\end{pmatrix} z_t + \begin{pmatrix}1&0&1\\0&0&1\\0&0&0\end{pmatrix} y_{t+1} + \begin{pmatrix}1&0&0\\0&1&0\\0&0&0\end{pmatrix} y_t, \quad \text{pour } t \geq 0.$$

Notez que M_0^{-1} est un transducteur fini quasi-linéaire avec mémoire d'ordre (0, 2) et M_1^{-1} est un transducteur linéaire fini à mémoire (2, 2). Le fait que M^{-1} soit un transducteur à entrée la mémoire est égale au délai de M_1, c'est la raison pour laquelle nous devons ajouter le texte en clair avec 2 symboles choisis arbitrairement.

Enfin, nous avons besoin des états initiaux de ces transducteurs. L'état initial de M_1^{-1} est $< y_0, y_1, z_0, z_1 >=$

$$< \lambda_0(< x_0, x_1 >, x_2), \lambda_0(< x_1, x_2 >, x_3), z_0, z_1 >=< \begin{pmatrix}0\\0\\0\end{pmatrix}, \begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix} >$$

et l'initiale l'état de M_0^{-1} est $< x_2, x_3 >$ (c'est évident si l'on remarque que la première entrée est x_4).

Exemple 5.2.2. Pour déchiffrer le texte chiffré calculé dans l'exemple précédent, le propriétaire du La clé publique n'a besoin que d'utiliser les inverses des transducteurs de la clé privée et les états initiaux respectifs. En premier lieu, il faut utiliser M_1^{-1} pour obtenir y_2 et y_3 :

$$y_2 = \lambda_1^{-1}(< y_0, y_1, z_0, z_1 >, z_2) = \lambda_1^{-1}\left(< \begin{pmatrix}0\\0\\0\end{pmatrix}, \begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix} >, \begin{pmatrix}1\\0\\1\end{pmatrix}\right) = \begin{pmatrix}0\\0\\1\end{pmatrix}.$$

$$y_3 = \lambda_1^{-1}(< y_1, y_2, z_1, z_2 >, z_3) = \lambda_1^{-1}\left(< \begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\1\end{pmatrix} >, \begin{pmatrix}1\\1\\0\end{pmatrix}\right) = \begin{pmatrix}0\\0\\0\end{pmatrix}.$$

Machine Translated by Google

Par conséquent, en utilisant M_0^{-1} on peut récupérer l'entrée α = x4x5 :

$$x_4 = \lambda_0^{-1}(\langle x_2, x_3\rangle, y_2) = \lambda_0^{-1}\left(\left\langle \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right\rangle, \begin{pmatrix}0\\1\end{pmatrix}\right) = \begin{pmatrix}1\\0\end{pmatrix}.$$

$$x_5 = \lambda_0^{-1}(\langle x_3, x_4\rangle, y_3) = \lambda_0^{-1}\left(\left\langle \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}\right\rangle, \begin{pmatrix}0\\0\end{pmatrix}\right) = \begin{pmatrix}0\\0\end{pmatrix}.$$

5.3 L'attaque de Bao-Igarashi

Bao et Igarashi ont prouvé, dans leur article [BI95], une propriété jusqu'alors inconnue des nombres finis inversibles. transducteurs. Grâce à cette propriété, ils réduisent le problème de séparation de M0 et M1 de la transducteur composé M = M1 ◦ M0 à un problème beaucoup plus simple : trouver un transducteur commun gauche spécial facteur de deux polynômes matriciels donnés dans des anneaux de polynômes matriciels modulaires. En gros, étant donné un transducteur à clé publique, cette propriété nous permet de trouver deux transducteurs finis M_0' et M_1' tel que, le transducteur inverse de $M' = M_1' \circ M_0'$, inverse également M.

Commençons par prouver une propriété des transducteurs finis inversibles : seuls les τ + 1 les plus récents les entrées déterminent si un transducteur est inversible avec un retard $\tau \in \mathbb{N}_0$. Il sera utilisé pour les transducteurs avec mémoire d'entrée uniquement, puisque le problème de la vérification de l'injectivité des transducteurs finis avec entrée et la mémoire de sortie peut être réduite au problème de vérification de l'injectivité des transducteurs avec τ+h mémoire d'entrée seule (Théorème 3.4.5). Soit $\tau, h \in \mathbb{N}_0$. Soit $M_f = \langle X, Y, X^{\tau+h}, \delta_f, \lambda_f\rangle$ et $M_{f+g} = \langle X, Y, X^{\tau+h}, \delta_{f+g}, \lambda_{f+g}\rangle$ soit une paire de transducteurs avec une mémoire d'entrée d'ordre τ + h, défini comme suit :

$$M_f : y_t = f(x_{t+\tau+h}, x_{t+\tau+h-1}, \ldots, x_t), \text{ pour } t \geq 0,$$

$$M_{f+g} : y_t = f(x_{t+\tau+h}, x_{t+\tau+h-1}, \ldots, x_t) + g(x_{t+h-1}, \ldots, x_t), \text{ pour } t \geq 0,$$

où $f : X^{\tau+h+1} \longrightarrow Y$ et $g : X^h \longrightarrow Y$. Notez que les τ + 1 entrées les plus récentes, $x_{t+\tau+h}, x_{t+\tau+h-1}, \ldots, x_{t+h}$, n'apparaissent que dans la fonction f.

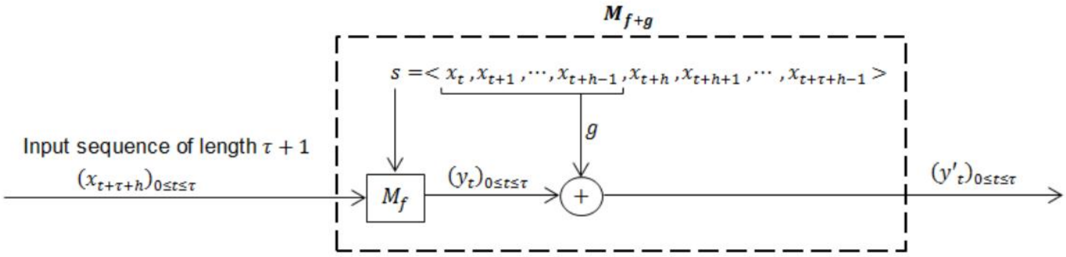


Figure 5.3 : Relation entre Mf et Mf+g

Théorème 5.3.1. Le transducteur fini Mf est inversible avec un retard τ si et seulement si Mf+g est inversible avec retard τ .

Preuve. Un transducteur M = X , Y, X τ+h ,δ, λ est τ -injectif si

s X τ+h , x, x X , α, α X τ , λ(s, xα) = λ(s, xα) = x = x .

Puisque, s =< x0, . . . , xh−1, xh, . . . , xh+τ−1 > X h+τ , x, x X , on a :

λf+g(s, x) = λf+g(s, x)

f(x, xτ+h−1, . . . , x0) + g(xh−1, . . . , x0) = f(x , xτ+h−1, . . . , x0) + g(xh−1, . . . , x0)

f(x, xτ+h−1, . . . , x0) = f(x , xτ+h−1, . . . , x0)

λf (s, x) = λf (s, x).

Pour prouver que x, x X , α, α X τ on a

λf+g(s, xα) = λf+g(s, xα) λf (s, xα) = λf (s, xα),

remarquez simplement que le mot d'entrée a une longueur τ + 1 donc, les entrées qui apparaissent dans la fonction g sont toutes partie de s, c'est-à-dire, sont constantes. Par conséquent, elles s'annulent dans λf+g(s, xα) = λf+g(s, xα) laissant avec λf (s, xα) = λf (s, xα).

Ainsi, Mf est inversible avec un délai τ si et seulement si Mf+g est inversible avec un délai τ . □

Ensuite, nous montrons qu'il est possible de construire un transducteur inverse de Mf+g à partir d'un transducteur inverse transducteur de Mf .

Soit M−1 = Y, X f , Y τ × X τ+h , δ−1 f , λ−1 f soit un transducteur inverse avec un retard τ de Mf . Soit s =< x0, x1, . . . , xτ+h−1 > soit l'état initial de Mf et xα X × X τ soit une séquence d'entrée. Si y = y0y1 . . . yτ Yτ+1 est la sortie de Mf , c'est-à-dire, y = λf (s, xα), et s −1 =

$< y_0, y_1, . . . , y_{\tau-1}, x_0, x_1, . . . , x_{\tau+h-1} >$, alors M_f^{-1} peut récupérer x car $x = \lambda_f^{-1} (s^{-1}, y_\tau)$.

La sortie $y' = y'_0 y'_1 . . . y'_\tau$ $Y^{\tau+1}$ de M_{f+g}, pour la même séquence d'entrée, est donné par

$$y'_t = y_t + g(x_{t+h-1}, . . . , x_t), \text{ pour } 0 \leq t \leq \tau.$$

Pour inverser M_{f+g}, étant donné y', il suffit de calculer $y_t = y'_t - g(x_{t+h-1}, . . . , x_t)$, $0 \leq t \leq \tau$ et d'utiliser M_f^{-1} pour récupérer x.

Le principe de construction de M_{f+g}^{-1} est illustré dans la figure suivante.

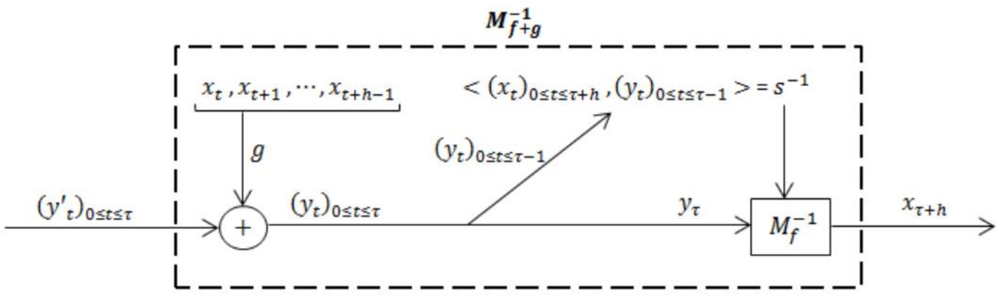


Figure 5.4 : Principe de construction de M_{f+g}^{-1}

Notez que, si l'on a deux transducteurs M_f et M_{f+g} dans les conditions précédentes, alors l'un on peut voir n'importe lequel d'entre eux comme le transducteur de base ou le transducteur étendu. Soit $M_{f'} = M_{f+g}$, c'est-à-dire $f' : X^{\tau+h+1} \longrightarrow Y$ tel que $f' = f + g$. On peut voir M_f comme $M_{f'+g'}$ où $g' : X^h \longrightarrow Y$ est tel que $g' = -g$.

Exemple 5.3.2. Soit $M_f = \langle \mathbb{F}_2^3, \mathbb{F}_2^3, \mathbb{F}_2^9, \mathbb{F}_2, \delta_f, \lambda_f \rangle$ soient le transducteur avec une mémoire d'entrée d'ordre 3 défini par :

$$y_t = f(x_{t+3}, x_{t+2}, x_{t+1}, x_t)$$
$$= \begin{pmatrix} 1&0&0\\0&1&0\\0&0&0 \end{pmatrix} x_{t+3} + \begin{pmatrix} 1&1&0\\0&1&0\\0&0&1 \end{pmatrix} x_{t+2} + \begin{pmatrix} 1&0&0\\0&1&0\\1&0&1 \end{pmatrix} x_{t+1} + \begin{pmatrix} 1&0&1\\0&1&1\\1&0&0 \end{pmatrix} x_t, \quad \text{pour } t \geq 0,$$

où $(x_t)_{t\geq 0}$ $\mathbb{F}_2^3$, $(y_t)_{t\geq 0}$ $\mathbb{F}_2^3$ et $f : \mathbb{F}_2^{12} \to \mathbb{F}_2^3$. M_f est inversible avec un retard de 1 et son inverse transducteur, $M_f^{-1} = \langle \mathbb{F}_2^3, \mathbb{F}_2^3, \mathbb{F}_2^{12}, \delta_f^{-1}, \lambda_f^{-1} \rangle$ est donné par :

$$x_{t+3} = \begin{pmatrix} 0&0&0\\0&0&0\\0&0&1 \end{pmatrix} y_{t+1} + \begin{pmatrix} 1&0&0\\0&1&0\\0&0&0 \end{pmatrix} y_t + \begin{pmatrix} 1&1&0\\0&1&0\\1&0&1 \end{pmatrix} x_{t+2} + \begin{pmatrix} 1&0&0\\0&1&0\\1&0&0 \end{pmatrix} x_{t+1} + \begin{pmatrix} 1&0&1\\0&1&1\\0&0&0 \end{pmatrix} x_t.$$

Soit $M_{f+g} = \langle \mathbb{F}_2^3, \mathbb{F}_2^3, \mathbb{F}_2^9, \delta_{f+g}, \lambda_{f+g} \rangle$ soit le transducteur avec mémoire d'entrée d'ordre 3 défini par :

$$y_t = \begin{pmatrix} 1&0&0 \\ 0&1&0 \\ 0&0&0 \end{pmatrix} x_{t+3} + \begin{pmatrix} 1&1&0 \\ 0&1&0 \\ 0&0&1 \end{pmatrix} x_{t+2} + \begin{pmatrix} 0&0&0 \\ 0&0&1 \\ 0&1&0 \end{pmatrix} x_{t+1} + \begin{pmatrix} 1&0&1 \\ 1&0&1 \\ 1&0&0 \end{pmatrix} x_t, \quad \text{pour } t \geq 0,$$

où $(x_t)_{t\geq 0} \in \mathbb{F}_2^3$ et $(y_t)_{t\geq 0} \in \mathbb{F}_2^3$. Si l'on considère $g : \mathbb{F}_2^6 \to \mathbb{F}_2^3$ où

$$g(x_t, x_{t+1}) = \begin{pmatrix} 1&0&0 \\ 0&1&1 \\ 1&1&1 \end{pmatrix} x_{t+1} + \begin{pmatrix} 0&0&0 \\ 1&1&0 \\ 0&0&0 \end{pmatrix} x_t,$$

alors $y_t = f(x_{t+3}, x_{t+2}, x_{t+1}, x_t) + g(x_t, x_{t+1})$, pour $t \geq 0$. Soit $s = \langle x_0, x_1, x_2 \rangle = \left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \right\rangle$

soit l'état initial de M_{f+g} (également l'état initial de M_f) et $\alpha = x_3 x_4 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ être la séquence d'entrée. La sortie de M_{f+g} est alors :

$$y_0 y_1 = \lambda_{f+g}(s, \alpha) = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}.$$

Puisque $y_t = y_t - g(x_t, x_{t+1})$, pour $t = 0, 1$, on a :

$$y_0 - g(x_0, x_1) = y_0 \; y_0 = -g\left(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

$$y_1 - g(x_1, x_2) = y_1 \; y_1 = -g\left(\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}.$$

Allons-y $s^{-1} = \langle y_0, x_0, x_1, x_2 \rangle$ soit l'état initial de M_f^{-1} et soit y_1 l'entrée. Alors la sortie est :

$$\lambda_f^{-1}(s^{-1}, y_1) = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = x_3.$$

De cette façon, on peut récupérer le symbole d'entrée x_3 de M_{f+g} en utilisant le transducteur inverse de M_f.

Nous sommes désormais en mesure de présenter l'attaque Bao-Igarashi au FAPKC.

Soit M_0 et M_1 les transducteurs dont les inverses sont dans la clé privée. Soit $M_0 = \langle X, Y, X^{h_0}, \delta_0, \lambda_0 \rangle$ soit un transducteur fini quasi-linéaire avec mémoire d'entrée h_0 et inversible avec un retard de 0 défini par

$$M_0 : y_t = \sum_{j=0}^{h_0} B_j x_{t+h_0-j} + \sum_{j=1}^{h_0-1} \tilde{B}_j x_{t+h_0-j} \cdot x_{t+h_0-j-1}, \text{ pour } t \geq 0,$$

où, pour un $\in \mathbb{N}$, $(B_j)_{0\leq j\leq h_0}, (\tilde{B}_j)_{1\leq j\leq h_0-1} \in M(\mathbb{F}_2)$ et B_0 est une matrice inversible. L'opération $\cdot$ est définie comme une multiplication par composantes, mais pourrait être toute autre opération non linéaire opération binaire. Notez que x_{t+h} n'apparaît que dans la partie linéaire de M_0. Il est facile de voir que le transducteur M_0^{-1}, avec mémoire d'ordre $(0, h)$, donnée par :

$$M_0^{-1} : x_{t+h_0} = B_0^{-1}\left(y_t + \sum_{j=1}^{h_0} B_j x_{t+h_0-j} + \sum_{j=1}^{h_0-1} \tilde{B}_j x_{t+h_0-j} \cdot x_{t+h_0-j-1}\right), \quad \text{pour } t \geq 0,$$

est un transducteur inverse avec un retard de 0 de M_0. Pour tout état initial $s_0 = \langle x_0, x_1, \ldots, x_{h-1} \rangle \in X^h$ de M_0, son état inverse dans M_0^{-1} est également $\langle x_0, x_1, \ldots, x_{h-1} \rangle$.

Soit $M_1 = \langle Y, Z, Y^{h_1}, \delta_1, \lambda_1 \rangle$ un transducteur linéaire à mémoire d'entrée h_1 et inversible avec retard $\tau \in \mathbb{N}$, défini par

$$M_1 : z_t = \sum_{i=0}^{h_1} A_i y_{t+h_1-i}, \text{ pour } t \geq 0 \text{ et } A_i \in M(\mathbb{F}_2).$$

Le transducteur composé $M = M_1 \circ M_0$ est obtenu en substituant $(y_t)_{t\geq 0}$ dans la définition de M_1 par ceux donnés par l'équation de M_0 (comme vu dans la section précédente).

$$M : z_t = \sum_{i=0}^{h_1} A_i \left(\sum_{j=0}^{h_0} B_j x_{t+h_0+h_1-j-i} + \sum_{j=1}^{h_0-1} \tilde{B}_j x_{t+h_0+h_1-j-i} \cdot x_{t+h_0+h_1-j-i-1}\right), \quad \text{pour } t \geq 0.$$

Cette équation peut être simplifiée comme suit :

$$M : z_t = \sum_{k=0}^{h_0+h_1} C_k x_{t+h_0+h_1-k} + \sum_{k=1}^{h_0+h_1-1} \tilde{C}_k x_{t+h_0+h_1-k} \cdot x_{t+h_0+h_1-k-1}, \text{ pour } t \geq 0,$$

où

$$C_k = \sum_{i+j=k} A_i B_j, \text{ pour } k = 0, 1, \ldots, h_0 + h_1 \text{ ; et}$$

$$\tilde{C}_k = \sum_{i+j=k} A_i \tilde{B}_j, \quad \text{pour } k = 1, 2, \ldots, h_0 + h_1 - 1.$$

En fait, l'attaque Bao-Igarashi ne fonctionne que lorsque le retard du transducteur M1 est tel que $\tau \leq h0$ et $\tau \leq h1 - 1$. Ici, on présentera une généralisation de l'attaque. Afin de pour cela, il faut étendre la mémoire d'entrée des transducteurs, avec autant de matrices nulles que nécessaire, pour que τ vérifie les conditions précédentes. Soit $M = X , Y, X^h, \delta, \lambda$ soit un nombre fini transducteur avec mémoire d'entrée h définie par

$$yt = \sum_{i=0}^{h} Aixt+h-i \text{ , pour } t \geq 0,$$

où $(xt)t\geq 0$ X , $(yt)t\geq 0$ Y et s =< x0, x1, . . . , xh−1 > est l'état initial. L'état étendu h transducteur M = X , Y, 0 × X dim(X)×1 , δ , λ avec une mémoire d'entrée d'ordre h + est donné par

$$yt = \sum_{i=0}^{h+} \text{Un } ixt+h+-i \text{ , pour } t \geq 0,$$

où A je = Ai pour i = 0, 1, . . . , h et A je = 0 pour i = h + 1, h + 2, . . . , h + , c'est-à-dire l'étendue le transducteur est défini par

$$yt = \sum_{i=0}^{h} Aixt+h+-i \text{ , pour } t \geq 0.$$

L'état initial de ce transducteur est également accompagné de vecteurs nuls, il est donc donné par < 0, . . . , 0, x0, x1, . . . , xh−1 > 0 × X dim(X)×1 h . Soit 0 =< 0, . . . , 0 > 0 dim(X)×1 . L'état la fonction de transition δ est définie comme suit

$$\delta\ (< 0, s >, x) =< 0, \delta(s, x) >, \text{ où } x \quad X \text{ et } s \quad X^h.$$

Il est évident que le transducteur M et le transducteur étendu M sont équivalents.

Exemple 5.3.3. Soit M = F 3 2 , F 3 6 2 , F 2 , δ, λ soit un transducteur fini avec mémoire d'ordre (2, 0) défini par

$$yt = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} xt+2 + \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} xt+1 + \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} xt \text{ , pour } t \geq 0,$$

où $(xt)t\geq 0$ F^3_2 , $(yt)t\geq 0$ F^3_2 et s0 =< x0, x1, x2 > est l'état initial. L'équivalent un transducteur avec une mémoire d'entrée d'ordre 5 est donné par

$$yt = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} xt+4 + \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} xt+3 + \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} xt+2 + \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} xt+1 + \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} xt \text{ ,}$$

où $(x_t)_{t\geq 0}$ F $^3_2$, $(y_t)_{t\geq 0}$ F $^3_2$ et $s_0 =< 0_{3\times 1}, 0_{3\times 1}, x_0, x_1, x_2 >$ est l'état initial du transducteur.

Soient A, B, B˜, C, C˜, les ensembles de matrices suivants dans les équations qui définissent les transducteurs M_0, M_1 et M, tels que présentés précédemment :

$$A = \{A_i : 0 \leq i \leq h_1\}, \qquad C = \{C_k : 0 \leq k \leq h_0 + h_1\},$$

$$B = \{B_j : 0 \leq j \leq h_0\}, \qquad \tilde{C} = \{\tilde{C}_k : 1 \leq k \leq h_0 + h_1 - 1\},$$

$$\tilde{B} = \{\tilde{B}_j : 1 \leq j \leq h_0 - 1\}.$$

Supposons que, pour les ensembles de matrices C et C˜, on puisse trouver un nouvel ensemble de matrices A $_{je}$: = {A 0 ≤ i ≤ τ}, B = {Bj : 0 ≤ j ≤ τ} (où B et C˜ $_0$ est inversible) et B˜ = {B˜ $_j$: 1 ≤ j ≤ τ} tel que Ck = i+j=k Un iB j , pour k = 0, 1, ..., τ , $_k$ = $_{i+j=k}$ Un iB˜ pour k = 1, ..., j , τ .

Il est facile de construire un transducteur fini quasi-linéaire, M $_0$, des ensembles B et B˜ . Ceci le transducteur est inversible avec un retard de 0, puisque B_0 est une matrice inversible. Il est également facile de construire un transducteur linéaire, M_1 , de A . On peut alors construire le transducteur M = M $_1$ ◦ M 0 .

$$M : z_t = \sum_{k=0}^{2\tau} C\ k x_{t+h_0+h_1-k} + \sum_{k=1}^{2\tau} \tilde{C}\ k x_{t+h_0+h_1-k} \cdot x_{t+h_0+h_1-k-1}, \text{ pour } t \geq 0,$$

où C $_k$ = $_{i+j=k\ \tau}$ iB j , pour k = 0, 1, . . . , 2τ et C˜ A $_k$ = $_{i+j=k}$ Un iB˜$_j$, pour k = 1, 2, . . . , 2τ . Puisque Ck = C k et C˜ pour k = 0, 1, . . . , $_k$ = C˜ $_k$ pour k = 1, 2, . . . , τ , les transducteurs M et M ont les mêmes matrices de coefficients pour les entrées τ + 1 les plus récentes. Cela signifie que, à partir de Théorème 5.3.1 et puisque M est inversible avec retard τ , M est également inversible avec un retard τ . Ainsi, comme illustré dans l'exemple 5.3.2, on peut construire un transducteur inverse avec un retard τ de M à partir de $M^{-1} = M^{-1}_0 \circ M^{-1}_1$.

Le problème de trouver de tels ensembles de matrices A , B et B˜ peuvent être résolus comme suit. Soit B $_0$ être la matrice identité et B j = 0 pour j = 1, 2, . . . , τ . Alors, puisque l'on veut Ck = i+j=k τ . On peut trouver Un iB j , il suffit de choisir A que C˜ $_{je}$ l'ensemble des matrices B˜ telles = Ci , pour i = 0, 1, ..., $_k$ = $_{i+j=k}$ Un iB˜$_j$ = $_{i+j=k}$ CiB˜$_j$, pour k = 1, ..., τ , en résolvant le système suivant de solutions linéaires équations

$$\begin{pmatrix} C_0 & 0 & \cdots & 0 \\ C_1 & C_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ C_{\tau-1} & C_{\tau-2} & \cdots & C_0 \end{pmatrix} \begin{pmatrix} \tilde{B}_1 \\ \tilde{B}_2 \\ \vdots \\ \tilde{B}_\tau \end{pmatrix} = \begin{pmatrix} \tilde{C}_1 \\ \tilde{C}_2 \\ \vdots \\ \tilde{C}_\tau \end{pmatrix}.$$

Ce système a certainement des solutions. En fait, une solution simple est obtenue en utilisant les faits que $\tilde{C}_k = \sum_{i+j=k} A_i \tilde{B}_j$ pour $k = 1, 2, \ldots, \tau$, et $C_k = \sum_{i+j=k} A_i B_j$, pour $k = 0, 1, 2, \ldots, \tau$, comme suit:

$$\begin{pmatrix} \tilde{C}_1 \\ \tilde{C}_2 \\ \vdots \\ \tilde{C}_\tau \end{pmatrix} = \begin{pmatrix} A_0 & 0 & \cdots & 0 \\ A_1 & A_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ A_{\tau-1} & A_{\tau-2} & \cdots & A_0 \end{pmatrix} \begin{pmatrix} \tilde{B}_1 \\ \tilde{B}_2 \\ \vdots \\ \tilde{B}_\tau \end{pmatrix} =$$

$$= \begin{pmatrix} A_0 & 0 & \cdots & 0 \\ A_1 & A_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ A_{\tau-1} & A_{\tau-2} & \cdots & A_0 \end{pmatrix} \begin{pmatrix} B_0 & 0 & \cdots & 0 \\ B_1 & B_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ B_{\tau-2} & B_{\tau-3} & \cdots & B_0 \end{pmatrix} \begin{pmatrix} B_0 & 0 & \cdots & 0 \\ B_1 & B_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ B_{\tau-2} & B_{\tau-3} & \cdots & B_0 \end{pmatrix}^{-1} \begin{pmatrix} \tilde{B}_1 \\ \tilde{B}_2 \\ \vdots \\ \tilde{B}_\tau \end{pmatrix} =$$

$$= \begin{pmatrix} C_0 & 0 & \cdots & 0 \\ C_1 & C_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ C_{\tau-1} & C_{\tau-2} & \cdots & C_0 \end{pmatrix} \begin{pmatrix} B_0 & 0 & \cdots & 0 \\ B_1 & B_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ B_{\tau-2} & B_{\tau-3} & \cdots & B_0 \end{pmatrix}^{-1} \begin{pmatrix} \tilde{B}_1 \\ \tilde{B}_2 \\ \vdots \\ \tilde{B}_\tau \end{pmatrix}.$$

Par conséquent, une solution du système est donnée par :

$$\begin{pmatrix} \tilde{B}_1 \\ \tilde{B}_2 \\ \vdots \\ \tilde{B}_{\tau-1} \end{pmatrix} = \begin{pmatrix} B_0 & 0 & \cdots & 0 \\ B_1 & B_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ B_{\tau-2} & B_{\tau-3} & \cdots & B_0 \end{pmatrix}^{-1} \begin{pmatrix} \tilde{B}_1 \\ \tilde{B}_2 \\ \vdots \\ \tilde{B}_{\tau-1} \end{pmatrix}.$$

Après avoir trouvé les ensembles de matrices $\mathcal{A}$, $\mathcal{B}$ et $\tilde{\mathcal{B}}$, on peut facilement casser le FAPKC en construisant un transducteur inverse du transducteur à clé publique M.

Exemple 5.3.4. Soit M = F et $^3_{2}, F^{3}_{2}, F^{12}_{2}$, δ, λ sont le transducteur à clé publique avec mémoire d'entrée 4 inversible avec retard 2 présenté dans la section précédente (exemple 5.2.1) et défini par

$$M : z_t = \begin{bmatrix}1&0&0\\0&1&0\\0&0&0\end{bmatrix} x_{t+4} + \begin{bmatrix}0&0&1\\0&1&0\\0&0&0\end{bmatrix} x_{t+3} + \begin{bmatrix}1&0&1\\0&1&0\\0&0&1\end{bmatrix} x_{t+2} + \begin{bmatrix}0&1&1\\0&0&1\\0&0&0\end{bmatrix} x_{t+1} + \begin{bmatrix}1&0&1\\0&0&0\\0&1&0\end{bmatrix} x_t$$

$$+ \begin{bmatrix}0&0&0\\0&0&1\\0&0&0\end{bmatrix} x_{t+3}x_{t+2} + \begin{bmatrix}1&0&0\\1&0&0\\0&0&0\end{bmatrix} x_{t+2}x_{t+1} + \begin{bmatrix}0&0&0\\0&0&1\\1&0&0\end{bmatrix} x_{t+1}x_t, \text{ pour } t \geq 0.$$

Puisque M est inversible avec un délai de 2, il faut étendre sa mémoire à 5, car M_0 doit avoir mémoire d'entrée d'ordre 2 et M_1 mémoire d'entrée d'ordre 3. Considérons donc M défini par

$$M : z_t = \begin{bmatrix}1&0&0\\0&1&0\\0&0&0\end{bmatrix} x_{t+5} + \begin{bmatrix}0&0&1\\0&1&0\\0&0&0\end{bmatrix} x_{t+4} + \begin{bmatrix}1&0&1\\0&1&0\\0&0&1\end{bmatrix} x_{t+3} + \begin{bmatrix}0&1&1\\0&0&1\\0&0&0\end{bmatrix} x_{t+2} + \begin{bmatrix}1&0&1\\0&0&0\\0&1&0\end{bmatrix} x_{t+1}$$

$$+ \begin{bmatrix}0&0&0\\0&0&1\\0&0&0\end{bmatrix} x_{t+4}x_{t+3} + \begin{bmatrix}1&0&0\\1&0&0\\0&0&0\end{bmatrix} x_{t+3}x_{t+2} + \begin{bmatrix}0&0&0\\0&0&1\\1&0&0\end{bmatrix} x_{t+2}x_{t+1}, \text{ pour } t \geq 0.$$

Il est facile de construire M_1 de $A_{0,1,2}$ UN Un depuis $A_j = C_j$, pour j = 0, 1, 2.

$$M_1 : z_t = \begin{bmatrix}1&0&0\\0&1&0\\0&0&0\end{bmatrix} y_{t+2} + \begin{bmatrix}0&0&1\\0&1&0\\0&0&0\end{bmatrix} y_{t+1} + \begin{bmatrix}1&0&1\\0&1&0\\0&0&1\end{bmatrix} y_t, \text{ pour } t \geq 0.$$

Pour construire M_0, il faut trouver les matrices $B_{0,1,2}$, B $\tilde{B}_1$, $\tilde{B}_2$. La matrice B_0 est le matrice d'identité, $B_{1,2}$ = 0, et $\tilde{B}_1$, $\tilde{B}_2$ sont obtenus en résolvant le système linéaire suivant :

$$\begin{bmatrix}C_0 & 0\\ C_1 & C_0\end{bmatrix}\begin{bmatrix}\tilde{B}_1\\ \tilde{B}_2\end{bmatrix} = \begin{bmatrix}\tilde{C}_1\\ \tilde{C}_2\end{bmatrix}.$$

Une solution du système est $\tilde{B}_1 = \begin{bmatrix}0&0&0\\0&0&1\\1&0&0\end{bmatrix}$ et $\tilde{B}_2 = \begin{bmatrix}0&0&0\\1&0&1\\0&0&0\end{bmatrix}$. Ainsi, M_0 est le transducteur avec une mémoire d'entrée d'ordre 3 définie par

$$M_0 : y_t = \begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix} x_{t+3} + \begin{bmatrix}0&0&0\\0&0&1\\1&0&0\end{bmatrix} x_{t+2}x_{t+1} + \begin{bmatrix}0&0&0\\1&0&1\\0&0&0\end{bmatrix} x_{t+1}x_t, \text{ pour } t \geq 0.$$

Le transducteur composé $M = M_0 \circ M_1$ est donné par :

$$M : z_t = \begin{bmatrix} 1&0&0 \\ 0&1&0 \\ 0&0&0 \end{bmatrix} x_{t+5} + \begin{bmatrix} 0&0&1 \\ 0&1&0 \\ 0&0&0 \end{bmatrix} x_{t+4} + \begin{bmatrix} 1&0&1 \\ 0&1&0 \\ 0&0&1 \end{bmatrix} x_{t+3} + \begin{bmatrix} 0&0&0 \\ 0&0&1 \\ 0&0&0 \end{bmatrix} x_{t+4}x_{t+3}$$

$$+ \begin{bmatrix} 1&0&0 \\ 1&0&0 \\ 0&0&0 \end{bmatrix} x_{t+3}x_{t+2} + \begin{bmatrix} 1&0&0 \\ 1&0&0 \\ 1&0&0 \end{bmatrix} x_{t+2}x_{t+1} + \begin{bmatrix} 0&0&0 \\ 1&0&1 \\ 0&0&0 \end{bmatrix} x_{t+1}x_t, \quad \text{pour } t \geq 0.$$

Notez que les transducteurs M et M ont les mêmes matrices de coefficients pour les 3 plus récents entrées, c'est-à-dire $z_t = z_t + g(x_{t+2}, x_{t+1}, x_t)$, pour $t \geq 0$, où

$$g(x_{t+2}, x_{t+1}, x_t) = \begin{bmatrix} 0&1&1 \\ 0&0&1 \\ 0&0&0 \end{bmatrix} x_{t+2} + \begin{bmatrix} 1&0&1 \\ 0&0&0 \\ 0&1&0 \end{bmatrix} x_{t+1} + \begin{bmatrix} 1&0&0 \\ 1&0&1 \\ 0&0&0 \end{bmatrix} x_{t+2}x_{t+1} + \begin{bmatrix} 0&0&0 \\ 1&0&1 \\ 0&0&0 \end{bmatrix} x_{t+1}x_t.$$

Cela signifie que l'on est dans les conditions d'appliquer le théorème 5.3.1, qui permet d'inverser M d'un transducteur inverse de M . Pour inverser M il suffit de calculer $M^{-1} = M^{-1} \circ M_0^{-1}$. Soit $M^{-1} = F^{3}_{2,2,2}, F^{3}_{2,2,2}, \delta^{-1}, \lambda^{-1}$ soit un transducteur inverse de M défini par

$$M^{-1} : x_{t+5} = \begin{bmatrix} 0&0&0 \\ 0&0&0 \\ 0&0&1 \end{bmatrix} z_{t+2} + \begin{bmatrix} 1&0&0 \\ 0&1&0 \\ 0&0&0 \end{bmatrix} z_t + \begin{bmatrix} 0&0&1 \\ 0&1&0 \\ 0&0&0 \end{bmatrix} x_{t+4} + \begin{bmatrix} 1&0&1 \\ 0&1&0 \\ 0&0&0 \end{bmatrix} x_{t+3}$$

$$+ \begin{bmatrix} 0&0&0 \\ 0&0&1 \\ 1&0&0 \end{bmatrix} x_{t+4}x_{t+3} + \begin{bmatrix} 1&0&0 \\ 1&0&0 \\ 0&0&0 \end{bmatrix} x_{t+3}x_{t+2} + \begin{bmatrix} 1&0&0 \\ 1&0&0 \\ 0&0&0 \end{bmatrix} x_{t+2}x_{t+1} + \begin{bmatrix} 0&0&0 \\ 1&0&1 \\ 0&0&0 \end{bmatrix} x_{t+1}x_t.$$

Rappelons que, d'après l'exemple 5.2.1, l'état initial du transducteur M est $s = \left\langle \begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix} \right\rangle$.

Comme M a été étendu, son état initial est $s = \langle 0, x_0, x_1, x_2, x_3 \rangle = \left\langle \begin{bmatrix}0\\0\end{bmatrix}, \begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix} \right\rangle$.

Étant donné le texte chiffré $z_0z_1z_2z_3 = \begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}0\\0\end{bmatrix}\begin{bmatrix}1\\1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}$, et parce que M est inversible avec un délai de 2, l'état initial de M^{-1} est $s^{-1} =< z_0, z_1, 0, x_0, x_1, x_2, x_3 >$, où

$$z_0 = z_0 + g(x_1, x_0, 0) = \begin{pmatrix}1\\0\end{pmatrix} + g\left(\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\0\end{pmatrix}\right) = \begin{pmatrix}1\\0\end{pmatrix} + \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix},$$

$$z_1 = z_1 + g(x_2, x_1, x_0) = \begin{pmatrix}0\\0\end{pmatrix} + g\left(\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}\right) = \begin{pmatrix}0\\0\end{pmatrix} + \begin{pmatrix}1\\1\end{pmatrix} = \begin{pmatrix}1\\1\end{pmatrix}.$$

Pour décrypter z_2z_3, il faut procéder comme suit : calculer le z_2 à partir de z_2, récupérez x_4 en utilisant le transducteur M^{-1}, et répétez la procédure jusqu'à z_3.

$$z_2 = z_2 + g(x_3, x_2, x_1) = \begin{pmatrix}1\\1\end{pmatrix} + g\left(\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}\right) = \begin{pmatrix}1\\1\end{pmatrix} + \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}.$$

$$x_4 = \lambda^{-1}(< z_0, z_1, 0, x_0, x_1, x_2, x_3 >, z_2) = \begin{pmatrix}1\\0\end{pmatrix}.$$

$$z_3 = z_3 + g(x_4, x_3, x_2) = \begin{pmatrix}1\\0\end{pmatrix} + g\left(\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right) = \begin{pmatrix}1\\0\end{pmatrix} + \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix}.$$

$$x_5 = \lambda^{-1}(< z_1, z_2, 0, x_1, x_2, x_3, x_4 >, z_3) = \begin{pmatrix}0\\0\end{pmatrix}.$$

Le texte en clair est récupéré, c'est-à-dire $x_4x_5 = \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}0\\0\end{pmatrix}$, est la bonne (comme on peut le confirmer avec Exemple 5.2.1).

Chapitre 6

Conclusion

Dans ce travail, nous avons présenté des concepts et des résultats connus sur les transducteurs finis généraux ainsi que sur les transducteurs finis à mémoire, linéaires et quasi-linéaires. Nous avons simplifié le langage utilisé par Tao et illustré les concepts avec une grande variété d'exemples. De plus, nous a étendu la définition des transducteurs finis quasi-linéaires à mémoire, présentée par Tao sans une justification au fait que les entrées les plus récentes n'apparaissent que dans la partie linéaire.

Nous avons formalisé la méthode de Tao pour vérifier l'injectivité des transducteurs finis linéaires avec mémoire, avec un algorithme qui permet d'obtenir simultanément un transducteur inverse. Nous avons également présenté un et condition suffisante à l'inversibilité des transducteurs finis linéaires à mémoire. Considérant la difficulté de cette procédure, nous avons illustré toutes les phases à travers un exemple simple. La même chose a été effectué sur des transducteurs finis quasi-linéaires, et tous les résultats ont été étendus à notre nouvelle définition.

Nous avons présenté une nouvelle formalisation des deux manières différentes de composer des transducteurs finis décrit par Tao, et a présenté des résultats concernant l'ordre de la mémoire et l'injectivité retard des transducteurs composés par rapport à ses facteurs. Nous avons donné une description générale de tous FAPKCs au moyen d'un schéma général, le seul que nous pouvons comprendre à travers les papiers nous avions accès. Pour ce schéma de base, nous avons présenté une procédure de génération de clés ainsi que la processus de cryptage et de décryptage. Enfin, nous avons présenté l'attaque Bao-Igarashi à FAPKC. Cette attaque n'a jamais été illustrée par un exemple, et les documents associés manquent de preuves complètes et des explications. Nous avons formalisé et étendu cette attaque à tous les cas impliquant des algorithmes linéaires inversibles. transducteurs avec un délai de 0, car l'attaque d'origine ne fonctionne que pour des cas particuliers. Nous avons également illustré cette attaque à travers un exemple.

Pour les travaux futurs, il sera important de comprendre les autres variantes de FAPKC, en particulier comment la génération de clés pourrait être effectuée. Après cela, il faudrait envisager la possibilité d'étendre la Attaque Bao-Igarashi sur d'autres schémas FAPKC. Il est concevable que cette attaque puisse être modifiée pour factoriser les transducteurs composés obtenus à partir de transducteurs avec un retard non nul. Bien que de nombreux les documents indiquent que les schémas FAPKC après FAPKC2 ne sont pas vulnérables à cette attaque, aucune preuve a été fournie jusqu'à présent. Une autre direction fondamentale de recherche est l'étude des non-transducteurs finis linéaires et leur inversibilité.

Annexe A

Nombre de vérifications nécessaires pour

Test d'inversibilité des transducteurs

Soit $M = X, Y, X^h \times Y^k, \delta, \lambda$ soit un transducteur fini à mémoire d'ordre (h, k). Considérant la structure particulière des transducteurs finis avec mémoire, il est plausible que le nombre de contrôles nécessaire pour voir si M est ω-injectif est inférieur à $\frac{|S|(|S|-1)}{2}$, où $S = X^h \times Y^k$. En fait, nous suspecter que M est ω-injectif si et seulement s'il existe un entier non négatif $\tau \leq h \dim(X)$ tel que M soit injectif avec un délai τ .

Tout d'abord, nous commençons par faire quelques tests pratiques avec un transducteur fini linéaire avec uniquement une mémoire d'entrée, car le problème de vérification de l'injectivité peut être réduit à ces transducteurs. Dans les premiers essais, nous vérifions la τ-injectivité pour tous les transducteurs finis linéaires possibles avec une mémoire d'entrée d'ordre h, pour h = 1, 2, 3, sur F_2 , c'est-à-dire tous les transducteurs possibles M tels que $M = F_2^2, F_2^2, (F_2^2)^h, \delta, \lambda$. Le les résultats obtenus sont résumés dans le tableau suivant.

	nombre de transducteurs τ-injectifs							pas ω-injectif	total	$\frac{\|S\|(\|S\|-1)}{2}$
	τ = 0	τ = 1	τ = 2	τ = 3	τ = 4	τ = 5	τ = 6			
h = 1	96	78	18	-	-	-	-	64	256	6
h = 2	1536	1248	654	234	72	-	-	352	4096	120
h = 3	24576	19968	10464	5262	2250	936	288	1792	65536	2016

Tableau A.1 : Injectivité des transducteurs $M = F_2^2, F_2^2, (F_2^2)^h, \delta, \lambda$, pour h = 1, 2, 3

Machine Translated by Google

D'après les résultats présentés, on peut voir que les transducteurs finis linéaires de la forme M = $F^2_2, F^2_2, F^{2\,h}_2$, δ, λ avec mémoire d'entrée h, pour h = 1, 2, 3, sont ω-injectifs si et seulement s'ils sont τ -injectif pour τ ≤ h dim(F^2_2) = 2h.

Soit N. Nous sommes capables de construire un transducteur fini linéaire générique M = F_2, F_2, F^{h}_2, δ, λ, avec une mémoire d'entrée d'ordre h N, qui est inversible avec un délai τ = h :

$$M : y_t = \begin{bmatrix} Id_{-1} & 0_{(-1)\times 1} \\ 0_{1\times(-1)} & 0 \end{bmatrix} x_{t+h} + \begin{bmatrix} 0_{(-1)\times 1} & Id_{-1} \\ 1 & 0_{1\times(-1)} \end{bmatrix} x_t, \quad \text{pour } t \geq 0.$$

Exemple A.1. Soit M = $F^4_2, F^4_2, F^{4\,2}_2$, δ, λ soit le transducteur fini linéaire avec mémoire de ordre 2 défini par :

$$M : y_t = \begin{bmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&0 \end{bmatrix} x_{t+2} + \begin{bmatrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{bmatrix} x_{t+1} + \begin{bmatrix} 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \\ 1&0&0&0 \end{bmatrix} x_t, \quad \text{pour } t \geq 0.$$

M est inversible avec un délai τ = 2 × 4 = 8.

Pour comprendre la construction de l'exemple générique, il faut remarquer que le coefficient La matrice de xt+h est sous forme réduite et ne comporte qu'une seule ligne nulle. Les informations manquantes dans cette matrice est liée à la dernière composante de xt+h. Si l'on applique une transformation Rb , la dernière ligne est décalé d'une matrice vers la gauche. Il est nécessaire d'effectuer des transformations h Rb pour entrer une ligne non nulle dans la matrice des coefficients de xt+h. La première ligne non nulle arrivant à cette matrice est égale à la première ligne, il faut donc appliquer une transformation Ra , en ajoutant la première ligne à la dernière. Après cette transformation, la matrice des coefficients de xt+h continue égale à celle initiale, mais dans la dernière ligne de la matrice de coefficients de xt apparaît la première ligne. Après encore h Rb transformations, cette ligne entre dans la matrice des coefficients de xt+h mais elle est annulée par sa deuxième ligne dans le Ra transformation. Ce processus est répété plusieurs fois, jusqu'à ce que la ligne [00 . . . 01] entre dans la première matrice, qui a maintenant son rang complet. Le transducteur est donc inversible avec un retard h.

La question est maintenant de savoir s'il est possible d'avoir d'autres matrices au lieu des matrices nulles qui augmenter le retard. Afin de tester cette hypothèse, nous considérons les transducteurs finis linéaires M = $F^3_2, F^3_2, F^{3\,h}_2$, δ, λ , pour h = 2, 3, et on remplace les matrices nulles par toutes les matrices possibles de dimension 3 sur F2. Ensuite, on vérifie l'injectivité des transducteurs. Les résultats obtenus sont dans le tableau suivant.

Machine Translated by Google

	nombre de transducteurs τ-injectifs		pas ω-injectif	total	$\frac{\lvert S\rvert(\lvert S\rvert-1)}{2}$
	τ ≤ 3h	τ > 3h			
h = 2	512	0	0	512	2016
h = 3	262144	0	0	262144	130816

Tableau A.2 : Injectivité d'un sous-ensemble de transducteurs $M = F_2^3, F_2^3, F_2^{3\,h}, \delta, \lambda$, pour h = 2, 3

D'après le tableau précédent, nous constatons qu'aucun des transducteurs générés n'a de retard supérieur à 3h.

Bien que les tests présentés ne soient peut-être pas statistiquement pertinents, nous ne trouvons aucun transducteur qui réfute notre affirmation. Pour les travaux futurs, il sera important de prouver ce résultat.

Références

[AMR12] Ivone Amorim, António Machiavelo et Rogerio Reis. Séries puissantes formelles et Inversibilité des transducteurs linéaires finis. Dans NCMA, pages 33–48, 2012.

[AMR14a] Ivone Amorim, António Machiavelo et Rogerio Reis. Comptage équivalent transducteurs finis linéaires utilisant une forme canonique. Dans la Conférence internationale sur Mise en œuvre et application des automates, pages 70–83. Springer, 2014.

[AMR14b] Ivone Amorim, António Machiavelo et Rogerio Reis. Sur l'inversibilité du fini transducteurs linéaires. RAIRO-Theoretical Informatics and Applications, 48(1):107–125, 2014.

[AMR14c] Ivone Amorim, António Machiavelo et Rogóerio Reis. Étude statistique sur le nombre des transducteurs finis linéaires injectifs. Préimpression arXiv arXiv:1407.0169, 2014.

[BI95] Feng Bao et Yoshihide Igarashi. Break Finite Automata Public Key Cryptosystem, pages 147–158. Springer Berlin Heidelberg, Berlin, Heidelberg, 1995.

[dCA16] Ivone de F´atima da Cruz Amorim. Transducteurs finis linéaires vers une clé publique système cryptographique. 2016.

[Dif88] Whitfield Diffie. Les dix premières années de la cryptographie à clé publique. Actes de la IEEE, 76(5):560–577, 1988.

[ElG85] Taher ElGamal. Un cryptosystème à clé publique et un système de signature basé sur des clés discrètes logarithmes. IEEE transactions on information theory, 31(4):469–472, 1985.

[Kob87] Neal Koblitz. Cryptosystèmes à courbes elliptiques. Mathématiques du calcul, 48(177):203–209, 1987.

[McC71] Neal H. McCoy. Introduction à l'algèbre moderne. Allyn et Bacon, 1971.

[Mil85] Victor S Miller. Utilisation des courbes elliptiques en cryptographie. Dans Conférence sur la théorie et application des techniques cryptographiques, pages 417–426. Springer, 1985.

[Tao95] Renji Tao. Sur la transformation ra rb et l'inversion des automates finis composés. Rapport technique, Rapport technique n° ISCAS-LCS-95-10, Laboratoire d'informatique Sciences, Institut des logiciels, Académie chinoise des sciences, Pékin, 1995.

[Tao09] Renji Tao. Automates finis et application à la cryptographie. Springer, 2009.

[TC86] Renji Tao et Shihua Chen. Deux variétés de cryptosystèmes à clé publique à automates finis et les signatures numériques. Journal of Computer Science and Technology, 1(1):9–18, mars 1986.

[TC97] Renji Tao et Shihua Chen. Une variante du système de cryptographie à clé publique fapkc3. Journal des Réseaux et Applications Informatiques, 20(3):283 – 303, 1997.

[TC99] Renji Tao et Shihua Chen. La généralisation du cryptosystème à clé publique fapkc4. Bulletin scientifique chinois, 44(9) : 784–790, mai 1999.

[TCC97] Renji Tao, Shihua Chen et Xuemei Chen. Fapkc3 : Un nouvel automate public fini cryptosystème à clé. Journal of Computer Science and Technology, 12(4):289, juillet 1997.

[Val93] Robert J Valenza. Algèbre linéaire : une introduction aux mathématiques abstraites. Springer Médias scientifiques et commerciaux, 1993.