الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique

المدرسة العليا لأساتذة التعليم التكنولوجي -سكيكدة-
Ecole Normale Supérieure d'Enseignement Technologique, Skikda

Département de Mathématiques
et Informatique

قسم الرياضيات
والإعلام الآلي

مذكرة تخرج لنيل شهادة أستاذ تعليم متوسط

تزامن الأنظمة الديناميكية الفوضوية كأساس للتشفير الآمن

من إعداد
سالمي معز الدين
بوسقعة وائل

تحت إشراف
أ. بولعراس صالح

نوقشت من طرف
أ. عياش مصعب ..... رئيساً.
أ. قواسمية عقبة ..... مناقشاً.
أ. موس إلهام ..... مناقشاً.

2024/2025

ملخص

تهدف هذه المذكرة إلى دراسة العلاقة بين علم التشفير والأنظمة الديناميكية الفوضوية، وإبراز إمكانية استخدام الفوضى كأداة لتعزيز أمن المعلومات. في الفصل الأول، تطرقنا إلى المبادئ العامة لعلم التشفير وأنواعه المختلفة. أما الفصل الثاني، نخصص لدراسة خصائص الأنظمة الديناميكية والفوضوية، كالتحسس للشروط الابتدائية والسلوك غير الدوري. ثم تناولنا في الفصل الثالث مفهوم تزامن الأنظمة الفوضوية، والذي يمثل خطوة أساسية نحو استخدامها في التشفير. وأخيرًا، خُتمت المذكرة بتطبيق عملي تمثل في مزامنة نظام Chen باستخدام طريقة Carroll و Pecora ، مما يُبرز الجوانب التطبيقية للنظرية المدروسة.

تُظهر هذه الدراسة أن الأنظمة الفوضوية توفر آفاقًا واعدة في تطوير أنظمة تشفير معقدة وآمنة، وتشكل مجالًا مهمًا للبحث المستقبلي في تقاطع الرياضيات والتكنولوجيا.

الكلمات المفتاحية:

تشفير، أنظمة فوضوية، تزامن، أسس ليابونوف، أمن المعلومات، أنظمة ديناميكية.

❖ شكر وعرفان

إن الحمد لله نحمده ونستعينه ونستغفره، ونشكره سبحانه وتعالى على أن وفقنا لإتمام هذا العمل المتواضع، أما بعد: نتقدم بالشكر الجزيل والعرفان الجميل إلى الأستاذ المشرف صالح بولعراس الدي شرفنا بموافقته للإشراف على هذا البحث.

كما لا يفوتنا في هذا المقام أن نشكر أعضاء لجنة المناقشة لقبولهم مناقشة مذكرتنا.

ونتقدم بالشكر أيضا إلى كل طاقم المدرسة العليا لأساتذة التعليم التكنولوجي سكيكدة بإدارتها وأساتذتها.

وفي الأخير نشكر كل من ساهم في إنجاز هذا العمل المتواضع من قريب أو من بعيد ولو بكلمة طيبة.

❖ إهداء

بـــسم الله الرحمان الرحيم

إلى والدي حفظهما الله ورعاهما وأطال عمرهما....

إلى إخوتي الأعزاء، إلى جميع أساتذتنا الأفاضل....

إلى كل من ساهم في هذا العمل من قريب أو بعيد....

إلى أصدقاء القسم وأصدقاء الإقامة الجامعية....

نخصّ منهم أصدقاءنا في مسجد الطلبة الحدائق -1-

إليكم أهدي ثمرات هذا العمل المتواضع

سالمي معز الدين

❖ إهداء

إلى من كانت دعواتهم سرّ تقدّمي ونجاحي، إلى والدي الحبيب، الذي كان دومًا السند والداعم، وصاحب القلب الكبير... إلى والدتي الغالية، نبع الحنان، ومصدر العزيمة، التي لم تبخل عليّ يومًا بحبّها واحتوائها...

إلى أخي وأخواتي، الذين كانوا لي عونًا في كل المراحل، ورفاقًا في درب الحياة...

إلى أساتذتي الكرام، الذين غرسوا فيّ بذور العلم، وألهموني الطموح والسعي...

إلى كل صديق وفيّ، وكل من كان له أثر طيّب في هذه الرحلة...

أهدي هذا العمل المتواضع، عربون شكر ووفاء، ودعاءً بأن يُكتب في ميزان حسنات كل من ساعدني، ولو بكلمة.

"اللهم اجعل هذا العمل خالصًا لوجهك الكريم، ووفقني لما فيه الخير والنفع."

بوسقعة وائل

قائمة المحتويات

مقدمة 2

4 الفصل 1
عموميات حول علم التشفير

1.1 التاريخ الزمني لتطور تقنيات التشفير 5
2.1 مقدمة في علم التشفير 5
3.1 التشفير 6
1.3.1 فك التشفير 6
2.3.1 التشفير بالمفتاح العام 7
3.3.1 التشفير بالمفتاح السري 7
4.1 مبادئ كيركهوف (Kerckhoffs) في علم التشفير 9
5.1 أهداف علم التشفير 10
6.1 تصنيف الخوارزميات 11
1.6.1 أمثلة حول خوارزميات التشفير المتماثل 11
7.1 نظام التشفير بالمفتاح المتماثل 12
8.1 التشفير غير المتماثل 13
1.8.1 مزايا وعيوب التشفير غير المتماثل: 14
9.1 التشفير الهجين 15
10.1 التشفير التقليدي 16
1.10.1 التشفير عبر الاستبدال 17
2.10.1 التشفير عبر النقل 17
3.10.1 التشفير عبر الضرب 18

19 الفصل 2
الأنظمة الديناميكية الفوضوية

1.2 النظام الديناميكي 20
1.1.2 شعاع الحالة 21
2.1.2 فضاءات الطور (Espaces des phases) 21
3.1.2 التدفق (Flot) 21
2.2 المدار (Orbite) 22
3.2 نقاط التوازن (Points d'équilibre) 22
1.3.2 الجاذب (Attracteur) 23
2.3.2 الجاذب المنتظم 23
3.3.2 الجاذب الغريب 24
4.3.2 الإستقرار 24
4.2 مفهوم الاستقرار 25
1.4.2 الاستقرار بمفهوم ليابونوف Stabilité au sens de Lyapunov 25
5.2 خطّية الأنظمة الديناميكية 26
6.2 أسس ليابونوف 26
1.6.2 رقم ليابونوف 27
2.6.2 الطريقة الأولى لليابونوف (الطريقة غير المباشرة) 28
3.6.2 الطريقة الثانية لليابونوف (الطريقة المباشرة) 28
7.2 الفوضى 31
8.2 النظام الفوضوي 31
9.2 خصائص النظام الفوضوي 32
1.9.2 تطبيقات الفوضى 33
10.2 العلاقة بين التشفير والفوضى 33
11.2 أمثلة على الأنظمة الفوضوية 34

الفصل 3
تزامن الأنظمة الفوضوية

37

1.3 تزامن الأنظمة الفوضوية 38
1.1.3 تعريف التزامن 38
2.1.3 معيار راوث-هورفيتز (Routh-Hurwitz) 39
2.3 فئات التزامن 40
1.2.3 التزامن بالاقتران أحادي الاتجاه 40
2.2.3 التزامن بالاقتران ثنائي الاتجاه 40
3.3 أنواع التزامن 40
1.3.3 التزامن المتماثل 41
4.3 التزامن باستخدام طريقة التحكم المستمر 43
5.3 مبدأ التزامن المطابق 43
1.5.3 التزامن بطريقة كارول وبيكورا 45
6.3 التزامن المعمم (GS Generalized-Synchronization) 47
1.6.3 كشف واستقرار التزامن المعمم 48

49 الفصل 4
تطبيق

1.4 التزامن المطابق لنظام Chen باستخدام طريقة Carroll وPecora 50
1.1.4 نظام Chen 50
2.1.4 عندما يكون الإشارة المُرسِلة هي x 51
3.1.4 عندما تكون فيها الإشارة المُرسِلة هي y 53
4.1.4 عندما تكون الإشارة المُرسِلة هي z 54

قائمة الأشكال

1.1 مبدأ التشفير وفك التشفير 8
2.1 التشفير المتماثل 13
3.1 التشفير غير المتماثل 14
4.1 التشفير الهجين 16
5.1 المجال المدرج في التشفير 16
6.1 الاستبدال أحادي الحرف 17
7.1 التشفير عبر النقل 18

1.2 مخطط التشعب لنظام روسلر 30
2.2 مخطط التشعب لنظام هينون 31
3.2 جاذب نظام لورينز في معلم ثلاثي الأبعاد $\sigma = 10, b = 8/3, r = 28$ 35
4.2 السلسلة الزمنية $x(t), y(t), z(t)$ لنظام لورينز $\sigma = 10, b = 8/3, r = 28$ 36

1.4 التزامن المطابق لنظام Chen عندما يكون x هو الإشارة المرسِلة. 52
2.4 التزامن المطابق لنظام Chen عندما يكون y هو الإشارة المرسِلة. 54
3.4 التزامن المطابق لنظام Chen عندما يكون z هو الإشارة المرسِلة. 55

مقدمة

في عصر تتسارع فيه وتيرة التحول الرقمي وانتقال المعلومات، أصبح أمن البيانات من أبرز التحديات التي تواجه الأفراد والمؤسسات على حدّ سواء. ومع ازدياد الحاجة إلى حماية الخصوصية وضمان سرية المعطيات، برز علم التشفير كأداة أساسية لضمان أمن المعلومات، حيث يُعنى بتحويل البيانات إلى شكل غير قابل للفهم إلا من طرف من يملك مفتاحًا لفك تشفيرها. وقد تطور هذا العلم عبر العصور، من طرق بسيطة قديمة إلى خوارزميات معقدة تعتمد على أسس رياضية متينة، ويُعد اليوم حجر الزاوية في مجالات متعددة كالمعاملات البنكية، والاتصالات الرقمية.

في السنوات الأخيرة، ظهرت توجهات جديدة في علم التشفير تعتمد على مفاهيم غير تقليدية، من أبرزها الأنظمة الديناميكية الفوضوية. هذه الأنظمة، التي تتميز بحساسية مفرطة للشروط الابتدائية وسلوك معقد غير دوري، أظهرت قدرة عالية على إنتاج إشارات معقدة يصعب التنبؤ بها أو إعادة توليدها، وهو ما يجعلها مرشحة قوية لتوظيفها في التشفير.

الفوضى، رغم مظهرها العشوائي، تخضع لقوانين رياضية دقيقة ما يمنحها مزايا فريدة تمزج بين العشوائية والقدرة على التحكم.

ومن أجل توظيف هذه الأنظمة في التطبيقات الأمنية، برز مفهوم تزامن الأنظمة الفوضوية، والذي يتمثل في جعل نظامين أو أكثر يتصرفان بشكل متزامن رغم فوضويتهما. هذا التزامن يُعد خطوة ضرورية في بناء أنظمة تشفير تعتمد على الفوضى، حيث يُمكن من خلاله تمرير معلومات مشفّرة عبر قناة فوضوية ليتم فك تشفيرها في الطرف المستقبل عبر تزامن دقيق بين المرسل والمستقبل.

انطلاقًا من هذا السياق، تهدف هذه المذكرة إلى استكشاف الإمكانات التي توفرها الأنظمة الفوضوية في مجال التشفير، من خلال دراسة نظرية وعملية لتزامن نظام Chen باستعمال طريقة Carroll و Pecora ، ضمن مسعى لفهم العلاقة بين هذه المجالات المتداخلة، وفتح آفاق جديدة لتطوير أنظمة تشفير أكثر أمانًا وفعالية.

نتاج ذلك كان مذكرة مقسمة إلى ثلاث فصول على النحو التالي:

الفصل الأول: والمعنون بعموميات حول علم التشفير، تناولنا فيه استعراضًا شاملاً لمجال التشفير، بدءًا من جذوره التاريخية التي أدت إلى تطور تقنياته. ثم انتقلنا إلى استعراض مبادئه الجوهرية.

الفصل الثاني: تطرقنا فيه إلى الأنظمة الديناميكية ونقاط التوازن ثم إلى الفوضى وعلاقتها بالتشفير وبعض الأمثلة عن الأنظمة الديناميكية الفوضوية.

الفصل الثالث: تناولنا في هذا الفصل تزامن الأنظمة الفوضوية، فئات وأنواع التزامن من بينها التزامن المتماثل والتزامن باستخدام طريقة التحكم المستمر.

الفصل الرابع: تناولنا في هذا الفصل تطبيق التزامن المطابق لنظام Chen باستخدام طريقة Carroll وPecora.

الفصل 1

عموميات حول علم التشفير

1.1 التاريخ الزمني لتطور تقنيات التشفير 5
2.1 مقدمة في علم التشفير..... 5
3.1 التشفير 6
4.1 مبادئ كيركهوف (Kerckhoffs) في علم التشفير..... 9
5.1 أهداف علم التشفير..... 10
6.1 تصنيف الخوارزميات..... 11
7.1 نظام التشفير بالمفتاح المتماثل..... 12
8.1 التشفير غير المتماثل 13
9.1 التشفير الهجين 15
10.1 التشفير التقليدي 16

تزداد الحاجة إلى الأمن في الحياة الواقعية باستمرار ومن هذا المنطلق، طوّر العديد من الباحثين أنظمة تشفير لتلبية هذه المتطلبات. عند الحديث عن "التشفير"، تبرز العديد من التفسيرات، إذ غالبًا ما يُنظر إليه على أنه علم غامض، لا يُستخدم إلا من قبل الحكومات ويصعب فك رموزه، إلا من قِبل رياضيين بارعين.

الهدف الأساسي من علم التشفير هو تمكين طرفين من التواصل عبر قناة أكثر أمنًا، بحيث لا يتمكن أي طرف ثالث - حتى لو اعترض الرسالة - من فهم محتواها. قد تكون هذه القناة مثل خط هاتفي أو أي نوع من شبكات الاتصال الأخرى.

1.1 التاريخ الزمني لتطور تقنيات التشفير

يمر تاريخ التشفير بعدة مراحل رئيسية، يمكن تلخيصها على النحو التالي:

1. الحقبة الحرفية (1900م): تميزت هذه الفترة بالاستخدام البدائي لأساليب التشفير، حيث كان يُستبدل كل حرف في النص بحرف آخر يبعد عنه ثلاث خانات في الترتيب الأبجدي. تمثل هذه المرحلة الأساس لأنظمة الإبدال البسيطة.

2. الحقبة التقنية (من 1900 إلى 1970): شهدت هذه المرحلة تطورًا ملحوظًا باستخدام أجهزة ميكانيكية وكهروميكانيكية في عمليات التشفير، مثل آلة هاجلين (Hagelin) وآلة إنجما (Enigma) التي استخدمت بكثافة خلال الحرب العالمية الثانية.

3. الحقبة المعرفية (منذ نحو 30 عامًا): مع التقدم التكنولوجي، ظهرت آليات تشفير متقدمة قادرة على الإجابة عن أسئلة أمنية معقدة، مثل:
   * كيف يمكن تقديم خدمة آمنة دون وجود اتفاقية مسبقة على قناة يمكن التنصت عليها؟
   * كيف يمكن ضمان الموثوقية باستخدام معلومة سرية دون الكشف عن أي تفاصيل تتعلق بها؟

2.1 مقدمة في علم التشفير

يرجع أصل مصطلح "التشفير" (Cryptographie) إلى اللغة اليونانية، حيث يتكون من "kriptós" بمعنى "مخفي"، و"gráphein" بمعنى "الكتابة". ويُعرّف التشفير بأنه علم إخفاء المعلومات وجعلها غير قابلة للفهم من قِبل أي طرف غير مُصرّح له، باستثناء الشخص المُستهدَف بالرسالة، والذي يمكنه استرجاع المحتوى الأصلي بفضل امتلاكه للسر، والذي يُعرف بـ"المفتاح".

في علم التشفير الحديث، تعتمد عملية الإخفاء على تحوّلات رياضية تُعرف بالـ"خوارزميات التشفيرية" أو "أنظمة التشفير"، والتي تكون مرتبطة بطول المفتاح المستخدم. وتعتمد درجة أمان أي نظام تشفيري على عاملين أساسيين: قوة الخوارزمية المستخدمة، وطول المفتاح المعتمد. يتضمن علم التشفير تصميم آليات التشفير وفك التشفير، ويُمارَس من قِبل مختصين يُطلق عليهم "خبراء التشفير" أو "المُشفّرون".

3.1 التشفير

تعريف 1.3.1

هو العملية التي يتم فيها تحويل رسالة إلى شكل غير قابل للفهم من قبل أي طرف غير مخوّل.

1.3.1 فك التشفير

تعريف 2.3.1

هو العملية المعاكسة، وتهدف إلى استرجاع المعلومات الأصلية من النص المشفّر. يشير مصطلح "نظام التشفير" إلى كل من آليتَي التشفير وفك التشفير معًا. في هذا السياق:

*تُسمى المعلومات الأصلية غير المشفّرة "النص الواضح"، ويُرمز لها بـ M، وقد تكون سلسلة من البيانات، ملفًا نصيًا، تسجيلاً صوتيًا رقميًا، أو صورة رقمية. وبالنسبة للحاسوب، فإن M ما هي إلا بيانات ثنائية.

* أما "النص المشفّر"، والذي يُرمز له بـ C، فهو نتيجة تحويل M باستخدام مفتاح معين، ويكون عادةً في شكل بيانات ثنائية كذلك، وقد يكون مساويًا في الطول لـ M أو أطول منه.

يُرمز إلى دالة التشفير بالرمز E، حيث تقوم بتحويل النص الواضح M إلى النص المشفّر C اعتمادًا على مفتاح معين. يُعبَّر عن هذه العملية رياضيًا كما يلي:

$$E_k(M) = C,$$

حيث:

C: النص المشفّر (Ciphertext) .

M: النص الواضح (Plaintext) .

E_K: دالة التشفير باستخدام المفتاح K.

وعملية فك التشفير تستخدم دالة أخرى تُرمز لها بـ D، والتي تعيد النص المشفّر C إلى صورته الأصلية M باستخدام المفتاح ذاته (في حالة التشفير المتماثل) أو مفتاح مختلف (في حالة التشفير غير المتماثل)، ويُعبّر عن ذلك كما يلي:

$$D_K(C) = M.$$

الدالة العكسية والتي يُرمز لها بـ D هي دالة فك التشفير، وتقوم بتحويل النص المشفّر C إلى النص

الواضح M:

$$D(C) = M$$

وبما أن الهدف الأساسي من جميع هذه العمليات هو استرجاع النص الأصلي انطلاقًا من نسخته المشفّرة، فإنه ينبغي تحقق التوافق التالية:

$$D(E(M)) = M$$

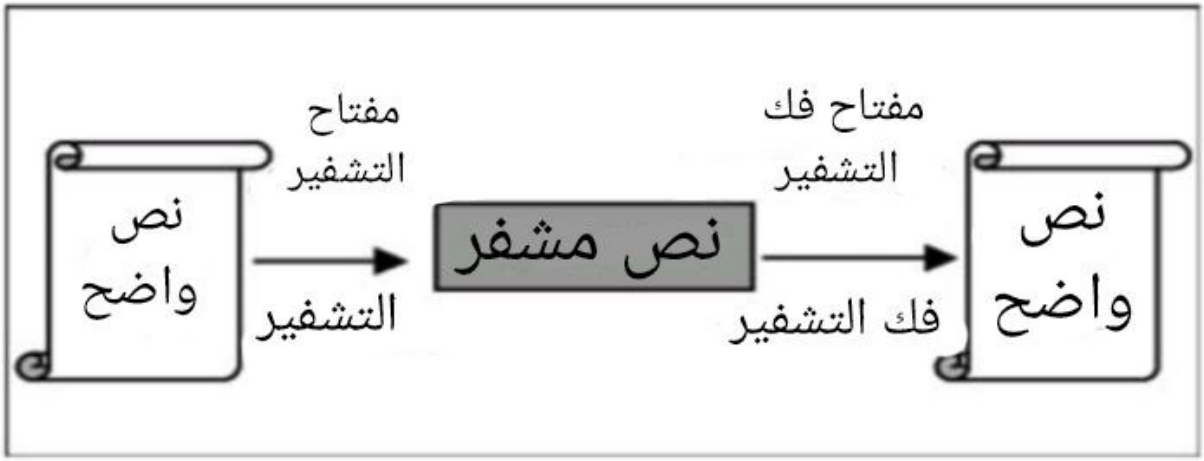
أي أن تطبيق دالة فك التشفير على نتيجة دالة التشفير يعيدنا إلى النص الأصلي. ومن بين مجموعة واسعة من تقنيات التشفير، تُمثل خوارزميتان اثنتان الركائز الأساسية في علم التشفير التقليدي:

2.3.1 التشفير بالمفتاح العام

يُعرف أيضًا بالتشفير غير المتماثل، ويعتمد على زوج من المفاتيح: مفتاح عام للتشفير،ومفتاح خاص لفك التشفير. يُستخدم المفتاح العام من قبل أي طرف لإرسال معلومات مشفّرة، في حين يبقى المفتاح الخاص سريًا لدى المتلقي فقط.

3.3.1 التشفير بالمفتاح السري

ويُعرف أيضًا بالتشفير المتماثل، حيث يُستخدم نفس المفتاح في عمليتي التشفير وفك التشفير. يتطلب هذا النظام أن يتفق الطرفان مسبقًا على مفتاح مشترك بطريقة آمنة لتبادل المفتاح بين الأطراف المعنية مسبقًا. سيتم تناول تفاصيل هذا النوع من التشفير في القسم التالي.



شكل 1.1: مبدأ التشفير وفك التشفير

المصطلحات:

النص الواضح: هو الرسالة الأصلية التي يُراد حمايتها.

النص المُشفر: هو نتيجة تطبيق عملية التشفير على النص الواضح.

التشفير: هو الطريقة أو الخوارزمية المستخدمة لتحويل نص واضح إلى نص مشفر.

فك التشفير: هو الطريقة أو الخوارزمية التي تُستخدم لتحويل النص المشفر إلى نص واضح.

المفتاح: هو السر المُشترك المستخدم في تشفير النص الواضح وفك تشفير النص المشفر. يمكن نظريًا تصميم خوارزمية لا تستخدم مفتاحًا خارجيًا، وفي هذه الحالة تكون الخوارزمية نفسها هي المفتاح، ويجب عدم الكشف عن مبدأ عملها.

دراسة التشفير: هو فرع يهتم بجميع الطرق التي تسمح بتشفير وفك تشفير النصوص الواضحة لجعلها غير مفهومة لمن لا يملك المفتاح المناسب.

تحليل التشفير: هو فن استرجاع النصوص الأصلية (الواضحة) من النصوص المشفرة دون معرفة المفتاح المستخدم.

علم التشفير: هو العلم الذي يدرس الاتصالات السرية، ويتكون من مجالين متكاملين لتشفير وتحليل التشفير.

فك التشفير: جعل الرسالة مفهومة مرة أخرى.

تشفير: إخفاء المعلومات أو جعلها غير مفهومة.

الترميز وفك الترميز: هي طريقة أو خوارزمية لتغيير شكل الرسالة دون إدخال عنصر سري. مثلا: يمكن تحويل الحروف إلى نقاط وخطوط دون أي سر في نظام مورس (Morse) ، أو إلى رموز رقمية باستخدام نظام ASCII .

تعريف 3.3.1 نظام التشفير

هو مجموعة المفاتيح الممكنة (فضاء المفاتيح)، والنصوص الواضحة والمشفرة الممكنة والمرتبطة بخوارزمية معينة. ويتكون فعليًا من ثلاث خوارزميات:

1. خوارزمية لتوليد المفاتيح K.
2. خوارزمية لتشفير الرسالة M.
3. خوارزمية لفك تشفير الرسالة C.

4.1 مبادئ كيركهوف (Kerckhoffs) في علم التشفير

تستند أنظمة التشفير المدنية المستخدمة حاليًا إلى المبدأ الأساسي التالي:
يجب ألا تعتمد أمانة التشفير على ما يمكن تغييره بسهولة. بعبارة أخرى، يجب ألا يكون هناك أي سر في الخوارزمية نفسها، بل ينبغي أن يكون السر في المفتاح. يجب أن يكون من المستحيل استرجاع النص الواضح من النص المشفّر دون المفتاح. أما إذا كان المفتاح معروفًا، فإن فك التشفير يكون فوريًا. يُعد هذا المبدأ واحدًا من المبادئ الستة التي نشرها كيركهوف في معاهده عن التشفير العسكري، والتي يمكن تلخيصها كالتالي:

1. لا ينبغي أن يكون من الممكن فك تشفير المعلومات المشفرة دون معرفة المفتاح.
2. يجب ألا يتعرض الأطراف المتعاملون لأي أضرار في حال تم الكشف عن نظام التشفير.
3. يجب أن يكون المفتاح بسيطًا وقابلًا للتعديل حسب الحاجة.
4. يجب أن تكون الرموز قابلة للتطبيق في المراسلات التلغرافية.
5. يجب أن تكون أجهزة التشفير والوثائق قابلة للنقل.
6. يجب أن يكون النظام سهل الاستخدام.

تفسير هذه المبادئ يعني أن السرية في الرسالة المشفرة يجب أن تعتمد على المعامل الذي يمكن تغييره بأقل تكلفة في حال تم الكشف عنه، وهو مفتاح فك التشفير.

5.1 أهداف علم التشفير

يشير مصطلح الأمن المعلوماتي إلى مجموعة الوسائل التي يتم تنفيذها لتقليل ضعف النظام ضد التهديدات العرضية أو المتعمدة. مفهوم الأمان يشير إلى خاصية نظام أو خدمة أو عنصر ما. يتم التعبير عن هذه الخاصية من خلال أهداف الأمان التي تُلخص في اختصار CAIN ، الذي يمثل:

1. السرية (Confidentialité) .
2. التحقق من الهوية (Authentfiication) .
3. النزاهة (Intégrité) .
4. عدم الإنكار (Non-répudiation) .

خواص:

السرية: فقط المستخدمون المصرح لهم يمكنهم الوصول إلى المعلومات. لضمان سرية البيانات، يجب تطبيق إجراءين مكملين:

1. تحديد البيانات والتحكم فيها لمنع أي تعديل غير مصرح به في حالة التشفير.
2. تحويل البيانات باستخدام تقنيات التشفير بحيث تصبح غير قابلة للفهم.

ففي حالة التشفير باستخدام المفتاح الخاص، يتم استخدام نفس المفتاح لكل من المرسل والمرسل إليه. أما في حالة التشفير باستخدام المفتاح العام، يكون لكل مستخدم زوج خاص به من المفاتيح. بينما في التشفير الهجين، فيتم استخدام التشفير بالمفتاح الخاص لتشفير الرسالة، ومن ثم تأمين تبادل المفتاح من خلال نظام التشفير بالمفتاح العام.

النزاهة: فقط المستخدمون المصرح لهم يمكنهم تعديل المعلومات. ومن هنا تبرز ضرورة التحقق من عدم تعرض الرسالة لأي تغييرات أثناء عملية التواصل.

التحقق من الهوية: هي الخاصية التي تتعلق بالتحقق من هوية المستقبل قبل منحه الإذن بالوصول إلى الموارد فيجب عليه إثبات هويته. جميع آليات التحكم في الوصول المنطقي إلى الموارد المعلوماتية تتطلب إدارة ومعرفة للتحقق من الهوية.

عدم الإنكار: وهي عدم القدرة على إنكار وقوع حدث (فعل، معاملة). ويحتوي على:

عدم إنكارالمصدر: لا يستطيع المرسل أن ينكر أنه كتب الرسالة، ويمكنه أن يثبت أنه لم يفعل ذلك إذا كان هذا هو الحال بالفعل.

عدم إنكارالاستلام: لا يستطيع المتلقي أن ينكر استلام الرسالة ويمكنه أن يثبت أنه لم يعيد استخدامها إذا كان هذا هو الحال بالفعل.

عدم إنكارالإرسال: لا يستطيع مرسل الرسالة أن ينكر إرسال الرسالة، ويمكنه أن يثبت أنه لم يفعل ذلك إذا كان الأمر كذلك بالفعل.

6.1 تصنيف الخوارزميات

يمكن تصنيف أنظمة التشفير وفقًا لعدة خصائص، منها:

1. حسب نوع المفاتيح: تشفير متماثل (Symmetric) ، غير متماثل (Asymmetric) ، أو هجين (Hybride) .
2. حسب تقنيات التشفير: تشفير بالكتل أو بالتدفق.
3. حسب العلاقة بين تدفق المفاتيح والنصوص: تشفير تزامني (synchrone) أو غير تزامني (asynchrone) .

1.6.1 أمثلة حول خوارزميات التشفير المتماثل

تعريف 1.6.1 معيار تشفير البيانات (DES) (Data Encryption Standard)

تُعد DES خوارزمية تشفير متماثلة تعتمد على معالجة كتل بيانات بطول 64 بايت، منها 8 بتات مخصصة لاختبار التماثل الفردي للمفتاح، ما يجعل الطول الفعلي للمفتاح المستخدم هو 56 بت.
يعتمد التشفير على سلسلة من التبديلات والاستبدالات بين النص والمفتاح، بطريقة قابلة للعكس لتيسير فك التشفير، ويُعرف هذا المزيج بـ "الشيفرة الناتجة" . يمثل المفتاح على 64 بتًا، يُشتق منه 16 مفتاحًا فرعيًا، يُستخدم كل منها في جولة من 16 جولة متتالية.
يتكوّن خوارزم DES من ثلاث مراحل رئيسية:

1. التموضع الابتدائي (Initial Permutation) .

2. 16 جولة معالجة (Feistel Rounds) تعتمد على المفتاح.

3. التموضع النهائي (Final Permutation) .

يبلغ عدد المفاتيح الممكنة: $2^{56} \approx 7.2 \times 10^{16}$.

تعريف 2.6.1 خوارزمية التشفير المتقدم (AES) (Advanced Encryption Standard)

تُعد أيضا AES خوارزمية تشفير متماثلة تعتمد على معالجة كتل بيانات بطول 128 بت (أي 16 بايت). يمكن أن يكون طول المفتاح المستخدم 128، 192 أو 256 بيت، وهو ما يحدد عدد جولات التشفير: 10، 12 أو 14 جولة على التوالي.
تُرتب البيانات في مصفوفة 4×4 بيت، وتخضع إلى عمليات والمراحل محددة تتكرر بحسب طول المفتاح، مما يضمن أمانًا عاليًا في التشفير ويمنع تحليل البنية الداخلية بسهولة.

7.1 نظام التشفير بالمفتاح المتماثل

تعريف 1.7.1

يعتمد التشفير المتماثل على استخدام نفس المفتاح السري من قبل الطرفين (المرسل والمستقبل) لتشفير وفك تشفير الرسالة. تنقسم خوارزميات هذا النوع إلى:

1. التشفير بالكتل: حيث تُقسم الرسالة إلى كتل ذات طول ثابت، وتُشفَّر باستخدام خوارزمية دورية تعتمد على مفتاح سري. من أشهر الأمثلة: DES و AES.

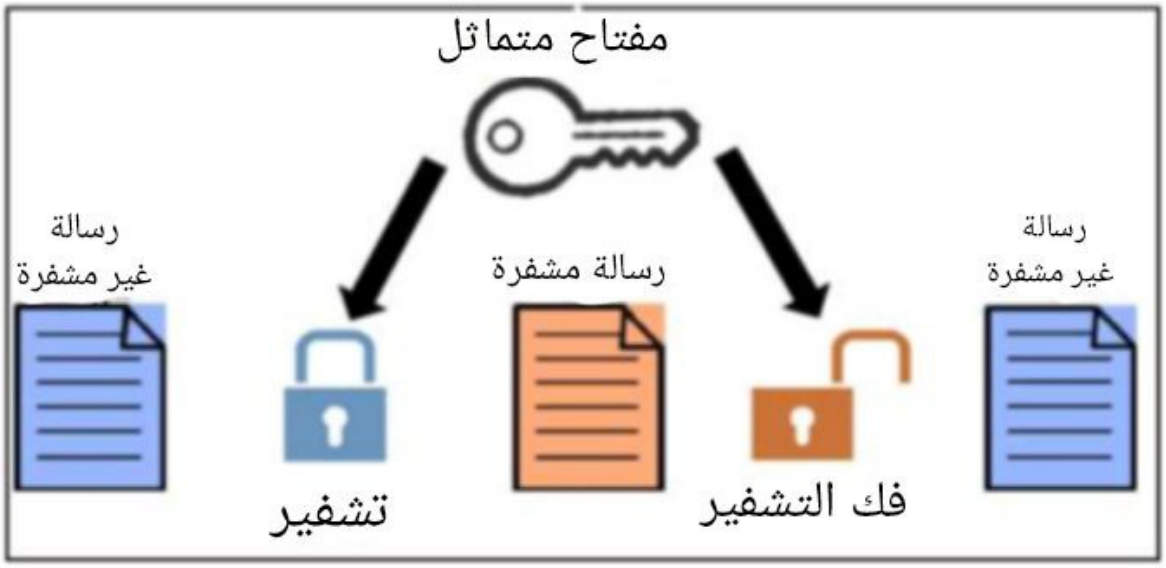
2. التشفير بالتدفق: يُشفَّر تيار البيانات باستخدام تدفق من المفاتيح يتغير بمرور الوقت.

مزاياه

1. سرعة الأداء.

2. سهولة التنفيذ (مفتاح واحد فقط).

3. إمكانية استخدامه كأساس لخوارزميات أخرى مثل الهاش.



شكل 2.1: التشفير المتماثل

عيوبه

1. الحاجة إلى عدد كبير من المفاتيح في الأنظمة متعددة المستخدمين.
2. صعوبة تأمين تبادل المفتاح السري.
3. عدم ضمان خاصية المصداقيـة.

8.1 التشفير غير المتماثل

يعتمد التشفير غير المتماثل على مسائل رياضية معقدة مثل تحليل الأعداد الصحيحة الكبيرة إلى عواملها الأولية أو حل معادلات اللوغاريتم المتقطع. ويرتكز هذا النوع من التشفير على مبدأ استخدام زوج من المفاتيح: مفتاح عام وآخر خاص. يُتاح المفتاح العام لأي شخص يرغب في تشفير رسالة، حيث يمكن للجميع معرفته، بينما لا يمكن فك تشفير الرسالة إلا باستخدام المفتاح الخاص، والذي يجب أن يبقى سريًا ولا يعرفه سوى مالكه.

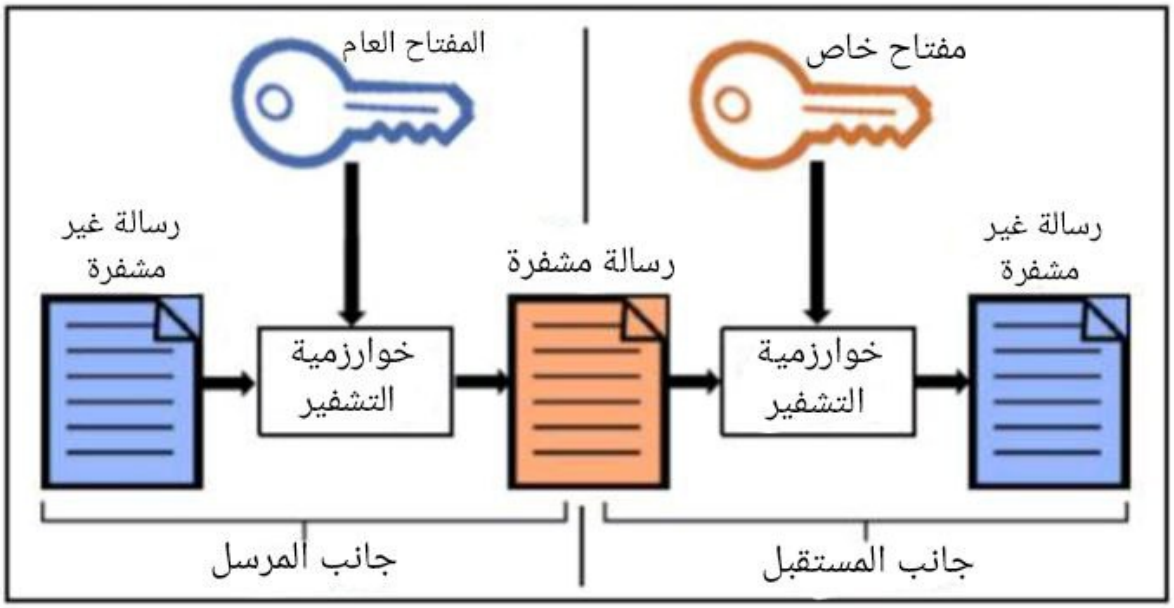
1.8.1 مزايا وعيوب التشفير غير المتماثل:

المزايا

1. التخلص من مشكلة تبادل المفاتيح السرية بين الأطراف.
2. إمكانية استخدام التوقيع الإلكتروني.
3. استحالة فك تشفير الرسالة في حال تم اعتراضها من طرف غير مخول.
4. إمكانية استخدام زوج المفاتيح (العام/الخاص) لفترة أطول مقارنة بمفتاح التشفير المتماثل.

العيوب

1. بطء الأداء مقارنة بالتشفير المتماثل.
2. احتمالية وقوع هجمات تعتمد على استبدال المفاتيح (مما يستلزم التحقق من هوية مصدر المفاتيح).
3. طول المفاتيح أكبر من نظيراتها في أنظمة التشفير المتماثل.



شكل 3.1: التشفير غير المتماثل

تعريف 1.8.1 دالة هاشاج (Hachage)

أو دالة التجزئة هي دالة رياضية أحادية الاتجاه تسمح بتشفير رسالة يستحيل فك تشفيرها بهدف ضمان سلامة البيانات والتأكد من أنها لم تتعرض لأي تعديل. مثلا في الاتصالات الآمنة عبر الإنترنت، غالباً ما يتم استخدام التشفير المختلط حيث يقوم المرسل بإنشاء مفتاح عشوائي متماثل لتشفير الرسالة، ويقوم بتشفيرها باستخدام المفتاح العام للمستلم.

خصائصها

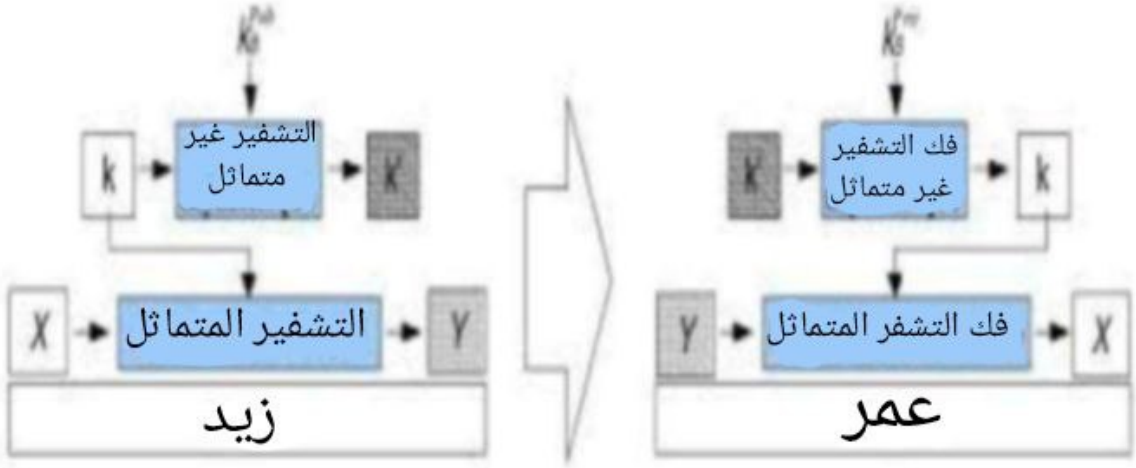
1. تولد صيغة فريدة لكل رسالة (تفادي التصادم).
2. ناتجها ذو حجم محدود وثابت.
3. لا يمكن استرجاع النص الأصلي (خاصية الاتجاه الواحد).

9.1 التشفير الهجين

تعريف 1.9.1

يهدف التشفير الهجين إلى الاستفادة من قوة كل من التشفير المتماثل وغير المتماثل:
يستخدم التشفير المتماثل لتشفير محتوى الرسالة لأنه أسرع.
وتُستخدم الطرق غير المتماثلة (المفتاح العام/الخاص) لتأمين تبادل المفتاح السري.
طريقة العمل:

1. يتم توليد مفتاح عشوائي (مفتاح الجلسة) لتشفير الرسالة باستخدام خوارزمية متماثلة.
2. يُشفَّر مفتاح الجلسة نفسه باستخدام المفتاح العمومي للمستقبِل.
3. يُرسل كلا من الرسالة المشفرة والمفتاح المشفر.
4. يقوم المستقبِل بفك تشفير مفتاح الجلسة باستخدام مفتاحه الخاص، ثم يستخدمه لفك تشفير الرسالة.

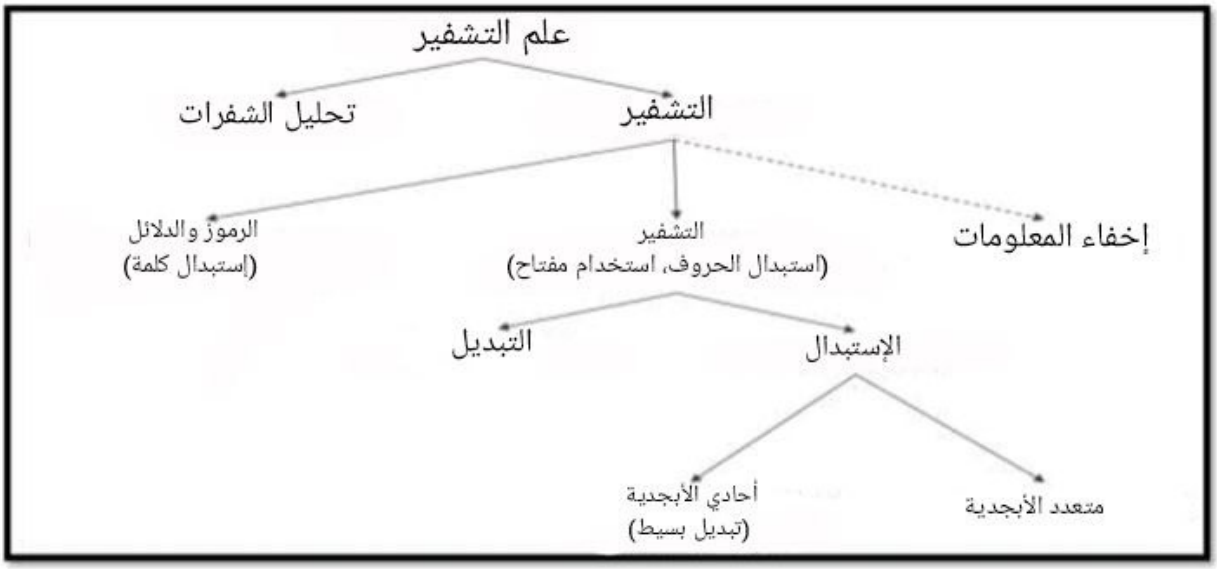


شكل 4.1: التشفير المجين

10.1 التشفير التقليدي

يمتد من العصر القديم إلى غاية ظهور الحواسيب, يضم كل الخوارزميات والآليات التي تعتمد على دوال رياضية أو منطقية. وتتم هذه الآلية عبر ثلاثة طرق:

1. التشفير عبر الاستبدال.
2. التشفير عبر النقل.
3. التشفير عبر الضرب.

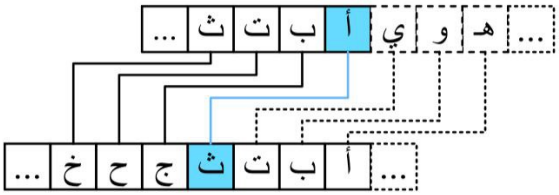


شكل 5.1: المجال المدرج في التشفير

1.10.1 التشفير عبر الاستبدال

حيث يتم استبدال عنصر واحد أو أكثر (عادةً أحرف) في رسالة بعنصر واحد أو أكثر آخر.
هناك عمومًا عدة أنواع من أنظمة التشفير عن طريق الاستبدال.

الاستبدال أحادي الحرف: حيث يتم استبدال كل حرف من الرسالة بحرف بتدرج معين.
مثال



شكل 6.1: الاستبدال أحادي الحرف

الاستبدال متعدد الحروف: حيث تستخدم متتالية من الشفرات أحادية الحرف معادة الاستخدام دوريا.

الاستبدال المتجانس: يسمح بمطابقة كل حرف من الرسالة الواضحة مع مجموعة محتملة من الأحرف الأخرى.

الاستبدال متعدد الرموز: عملية استبدال مجموعة واحدة من الرموز (متعدد الرموز) في الرسالة بمجموعة أخرى من الرموز.

2.10.1 التشفير عبر النقل

تتضمن طرق تشفير النقل إعادة ترتيب البيانات المراد تشفيرها بطريقة تجعلها غير مفهومة.
على سبيل المثال، يتضمن هذا إعادة ترتيب البيانات هندسيًا لجعلها غير قابلة للاستخدام بصريًا.
تُستخدم عدة أشكال من النقل، من بينها نجد:
النقل البسيط (المبني على المصفوفة): يتكون من كتابة النص الواضح في مصفوفة مكونة من n عمود (حرف واحد في كل خانة)، ثم إنشاء النص المشفر عن طريق أخذ الحروف من هذه المصفوفة عمودًا بعمود. المفتاح في هذه الحالة هو الرقم n.
النقل مع الاستبدال البسيط: الفكرة في هذه الحالة هي الجمع بين النقل والاستبدال البسيط. يتضمن ذلك تشفير الرسالة الواضحة باستخدام طريقة الاستبدال البسيطة، ثم تطبيق النقل. هناك خدعة أخرى تُستخدم بشكل متكرر وهي تطبيق دالة التبديل على ترتيب الأعمدة.

مثال

شكل 7.1: التشفير عبر النقل

3.10.1 التشفير عبر الضرب

وهو مزيج من تشفير الاستبدال وتشفير التبديل، وتستخدم هذا النوع من التشفير في معظم خوارزميات المفاتيح المتماثلة. نقول أن الحرف Z أصبح N قد اكتملت إذا تم إجراء التحويلين مرة واحدة (الاستبدال والنقل). وتسمى هذه العملية أيضا بشبكات S-P Shannon .

الفصل 2

الأنظمة الديناميكية الفوضوية

1.2 النظام الديناميكي 20
2.2 المدار (Orbite) 22
3.2 نقاط التوازن (Points d'équilibre) 22
4.2 مفهوم الاستقرار 25
5.2 خطّية الأنظمة الديناميكية 26
6.2 أسس ليابونوف 26
7.2 الفوضى 31
8.2 النظام الفوضوي 31
9.2 خصائص النظام الفوضوي 32
10.2 العلاقة بين التشفير والفوضى 33
11.2 أمثلة على الأنظمة الفوضوية 34

يعود مفهوم الزمن في دراسة النماذج الفيزيائية والرياضية إلى غاليليو (**Galiloeo**) ، الذي كان أول من أدخل هذا المفهوم في دراسة سقوط الأجسام وحركة الأرض حول الشمس. وسوف نطلق على هذه المقدمة للزمن في المعادلات اسم دراسة الأنظمة الديناميكية. في القرن الثامن عشر، حدد إسحاق نيوتن تكافؤ الكتلة والطاقة ووجد بشكل واضح سبب بعض الحركات غير المنتظمة على ما يبدو. ويتحدث عن الحتمية. وفقًا لهذا الرأي، يبدو أن كل شيء يمكن التنبؤ به وسببه تمامًا. يصبح المستقبل قابلاً للتنبؤ: يكفي ترجمة الحركة إلى معادلات تفاضلية وحلها.
بشكل عام، يصف النظام الديناميكي الظواهر التي تتطور بمرور الوقت. يشير مصطلح "نظام في النماذج الرياضية والفيزيائية إلى مجموعة من متغيرات الحالة، التي تتغير قيمتها بمرور الوقت، وإلى التفاعلات بين هذه المتغيرات.

1.2 النظام الديناميكي

تعريف 1.1.2

النظام الديناميكي هو كل نظام يتطور مع مرور الزمن، يُكرَّس لدراسة تقلبات حالة ظاهرة أو كائن معين. يمكن وصف هذا التطور بواسطة مجموعة محدودة من المعادلات التي يمكن أن تأخذ عدة أشكال رياضية: معادلات تفاضلية، أو معادلات تكرارية.

في حالة كون الزمن مستمراً :يتم تمثيل النظام الديناميكي بواسطة نظام من المعادلات التفاضلية على الشكل:

$$\frac{dX}{dt} = f(X, t, \mu), \quad X \in \Omega, \quad t \in \mathbb{R} \quad (2.1)$$

حيث:

$X \in \Omega \subseteq \mathbb{R}^n$ هو شعاع الحالة، و $\mu \in D \subseteq \mathbb{R}^p$ هو شعاع المعاملات.

$f : \Omega \times \mathbb{R} \times \mathbb{R}^p \to \mathbb{R}^n$ يُسمى حقل أشعة على Ω.

في الحالة المتقطعة، يُقدَّم النظام الديناميكي بواسطة دالة تكرارية:

$$X_{k+1} = f(X_k, u), \quad k \in \mathbb{N} \quad (2.2)$$

يُقال أن النظام (2.2) **غير ذاتي** إذا كان الزمن يظهر بشكل صريح في الدالة f، وفي الحالة المعاكسة يُقال أن النظام **ذاتي**.

ملاحظة : في هذه المذكرة نهتم بالأنظمة الديناميكية المستمرة.

نظرية 1.1.2

نظرية كوشي-ليبشيتز (Cauchy-Lipschitz)

لتكن لدينا مسألة كوشي:

$$\begin{cases} y'(t) = f(t, y(t))), & \forall t \in I, \\ y(t_0) = y_0. \end{cases}$$

إذا كانت الدالة f مستمرة على $I \times \mathbb{R}^d$ وفي نفس الوقت محققة لشرط ليبشيتز المحلي بالنسبة لـ y، فإن مسألة كوشي تقبل حلاً وحيدًا على المجال I.

1.1.2 شعاع الحالة

تعريف 2.1.2

نستعمل في دراسة الأنظمة الديناميكية مصطلح شائع هو شعاع الحالة و هو مجموعة المنحنيات الموجهة بأسهم و المتغيرة بدلالة الزمن t حيث يأخذ عدة أشكال تحدد لنا طبيعة نقطة التوازن حسب طبيعة القيم الذاتية للمصفوفة.

يُقدم النظام الديناميكي بواسطة نظام معادلات تفاضلية من الشكل: $\dot{x} = F(x,t,\lambda)$

حيث أن: $x \in \mathbb{R}^n$ هو شعاع الحالة، $\lambda \in \mathbb{R}^d$ هو شعاع المعاملات، و $F : \mathbb{R}^n \times \mathbb{R} \times \mathbb{R}^d$ يُسمى حقل الأشعة.

2.1.2 فضاءات الطور (Espaces des phases)

تعريف 3.1.2

في نظام ديناميكي ذو البُعد n ، يُسمى الفضاء $x_1, x_2, ...x_n$ فضاء الطور أو فضاء الحالة.

وبالتالي يُسمى المسار الذي يسلكه النظام "مداراً"، وتُمثل $x_1, x_2, ...x_n$ "حالات" النظام.

3.1.2 التدفق (Flot)

تعريف 4.1.2

لنأخذ النظام التالي:

$$\frac{dX}{dt} = f(X,t,\mu), \quad X \in \Omega, \quad t \in \mathbb{R} \quad (2.3)$$

وليكن $X(t,X_0), X_0 \in D$ حلاً للمعادلة (2.3) مع شرط ابتدائي $X(0) = X_0$. نطلق على تدفق النظام (2.3) اسم التطبيق: $\varphi_t : D \mapsto \mathbb{R}^n$ المعرف ب:

$$\varphi_t(X_0) = X(t,X_0),$$

$\varphi_t(X_0)$, يتمتع بالخصائص التالية:

1. $\varphi_t(X_0)$ من الصنف C^r ; $r \in \mathbb{N}$.

2. $\varphi_0(X_0) = X_0$.

3. $\varphi_{t+s}(X_0) = \varphi_t(\varphi_s(X_0))$.

2.2 المدار (Orbite)

تعريف 1.2.2

حل النظام (2.3) هو دالة $t \mapsto X(t)$ قابلة للاشتقاق معرفة على المجال $I \subset \mathbb{R}$ بحيث أنه من أجل كل $t \in I$، يكون:

$$\frac{dX}{dt} = f(X, t, \mu)$$

صورة هذا الحل X تُسمى مدارًا ويُرمز له بـ:

$$\{\delta \in \Omega; \exists t \in I : x(t) = \delta\}$$

المدار مماسي في كل نقطة من نقاطه إلى حقل الأشعة F.

3.2 نقاط التوازن (Points d'équilibre)

تعريف 1.3.2

نُسمي "نقطة التوازن" للنظام الديناميكي أي نقطة تحقق: $F(X_0) = 0$، أحيانًا تُسمى هذه النقاط أيضًا بالنقاط الثابتة أو النقاط المستقرة.

ملاحظة

عن طريق تغيير المتغير وفق العلاقة:

$$Y = X - X_0.$$

يمكننا تحويل النقطة X_0 إلى 0 .

1.3.2 الجاذب (Attracteur)

تعريف 2.3.2

الجاذب هو مجموعة في فضاء الطور تتقارب نحوها مسارات نظام ديناميكي مع الزمن. رياضيًا، نقول إن المجموعة A جاذب إذا تحققت الشروط التالية:

1. A مجموعة منتهية، مغلقة وثابتة تحت تأثير التدفق، أي:

$$\forall t \in \mathbb{R}, \quad \varphi_t(A) = A.$$

2. لكل جوار U لـ A، يوجد جوار V لـ A حيث كل حل $\varphi_t(X_0) = X(t, X_0)$ تبقى داخل U إذا كان $X_0 \in V$.

3. $\cap \varphi_t(V) = A, t \geq 0$

4. يوجد مسار كثيف في A.

يوجد نوعان من الجاذب: جاذب منتظم و جاذب غريب.

2.3.2 الجاذب المنتظم

الجاذبات المنتظمة تصف تطوّر الأنظمة غير الفوضوية، وتنقسم إلى ثلاثة أنواع رئيسية:

1. الجاذب النقطي (أو النقطة الثابتة): أبسط أنواع الجاذبات، حيث يتطور النظام نحو حالة سكون عند نقطة معينة في فضاء الطور.

2. الجاذب الدوري (أو الدورة الحدية): مسار مغلق في فضاء الطور، تتقارب نحوه المسارات الأخرى مع مرور الزمن.

3. الجاذب الطوري : يمثل حركة ناتجة عن تراكب تذبذبين مستقلين، وتكون المسارات فيه ملتفة حول طور.

3.3.2 الجاذب الغريب

الجاذبات الغريبة أكثر تعقيدًا من الأنواع السابقة، ويُطلق عليها هذا الاسم لأن أبعادها الكسرية (Fractales) غير صحيحة (ليست عددًا طبيعيًا)، وهو ما يبرّر وصفها بـ"الغريبة".
وتتميّز الجاذبات الغريبة بالخصائص التالية:

1. الحساسية الشديدة للشروط الابتدائية، أي أن تغيرًا بسيطًا في نقطة الانطلاق يؤدي إلى مسارات مختلفة جدًا.
2. حجمها معدوم في فضاء الطور.

4.3.2 الإستقرار

مقدمة

إن دراسة سلوك النظام الديناميكي المنفصل تعادل دراسة استقرار نقاط التوازن. سنتناول هنا فقط مشكلة نقاط توازنه، وبالنسبة للنقط الدورية للدورة p ، يكفي أن نأخذ في الاعتبار التكرار p للتطبيق.
لنفترض النظام الديناميكي غير الخطي:

$$\dot{x}(t) = F(x(t)),$$

بحيث أن الاستجابة هي:

$$x(t) = x(t, t_0, x(t_0)),$$

والشروط الأولية معرّفة بـ:

$$x(0) = x_0,$$

من أجل x_e نقطة توازن النظام، إذن:

$$F(x_e) = 0.$$

4.2 مفهوم الاستقرار

يُعدّ الاستقرار أحد الجوانب الأساسية في دراسة الأنظمة الديناميكية.
تُعدّ طريقة ليابونوف من الطرق الأساسية لتحليل استقرار الأنظمة الديناميكية.

1.4.2 الاستقرار بمفهوم ليابونوف Stabilité au sens de Lyapunov

تعريف 1.4.2

ليكن النظام الديناميكي التالي:

$$\frac{dX}{dt} = f(X,t), \quad X \in \Omega \subset \mathbb{R}^n, \quad t \in \mathbb{R} \quad (2.4)$$

حيث f دالة غير خطية.
نقطة التوازن X_0 للنظام (2.4) تكون:

1. مستقرة إذا تحقق الشرط التالي:

$$\forall \varepsilon > 0,\ \exists \delta > 0 : \|X(0) - X_0\| < \delta \Rightarrow \|X(t) - X_0\| < \varepsilon,\ \forall t \geq 0 \quad (2.5)$$

2. مستقرة بإنتظام إذا كانت X_0 مستقرة (بمفهوم ليابونوف)، و:

$$\exists \delta > 0 : \|X(0) - X_0\| < \delta \Rightarrow \lim_{t\to+\infty} \|X(t) - X_0\| = 0.$$

3. مستقرًا أسياً إذا وُجد عددان $\alpha > 0$ و $\beta > 0$ بحيث:

$$\forall \varepsilon > 0, \exists \delta > 0 : \|X(0) - X_0\| < \delta \Rightarrow \|X(t) - X_0\| < \alpha \|X(0) - X_0\| e^{-\beta t}. \quad \forall t \geq t_0$$

4. غير مستقرة: إذا لم تتحقق المعادلة (2.5).

5.2 خطّية الأنظمة الديناميكية

نعتبر النظام الديناميكي غير الخطي التالي:

$$\dot{X} = f(X), \quad X = (x_1, x_2, ..., x_n); f = (f_1, f_2, ..., f_n) \quad (2.6)$$

ولتكن X_0 نقطة توازن للنظام، ونفترض أن تغييرًا صغيرًا $\varepsilon(t)$ قد طُبِّق في جوار نقطة ثابتة.
بتطبيق نشر تايلور لـ f بجوار النقطة X_0 ، نحصل على:

$$\dot{\varepsilon}(t) + \dot{X}_0 = f(\varepsilon(t) + X_0) \approx f(X_0) + J_f(X_0)\varepsilon(t). \quad (2.7)$$

حيث أن:

$$Jf(X_0) = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_n}{\partial x_1} & \cdots & \frac{\partial f_n}{\partial x_n} \end{pmatrix}_{X=X_0} . \quad (2.8)$$

وهذه هي مصفوفة جاكوبي (Jacobienne) لـ f .
بما أن: $f(X_0) = 0$ فإن المعادلة (2.7) تصبح:

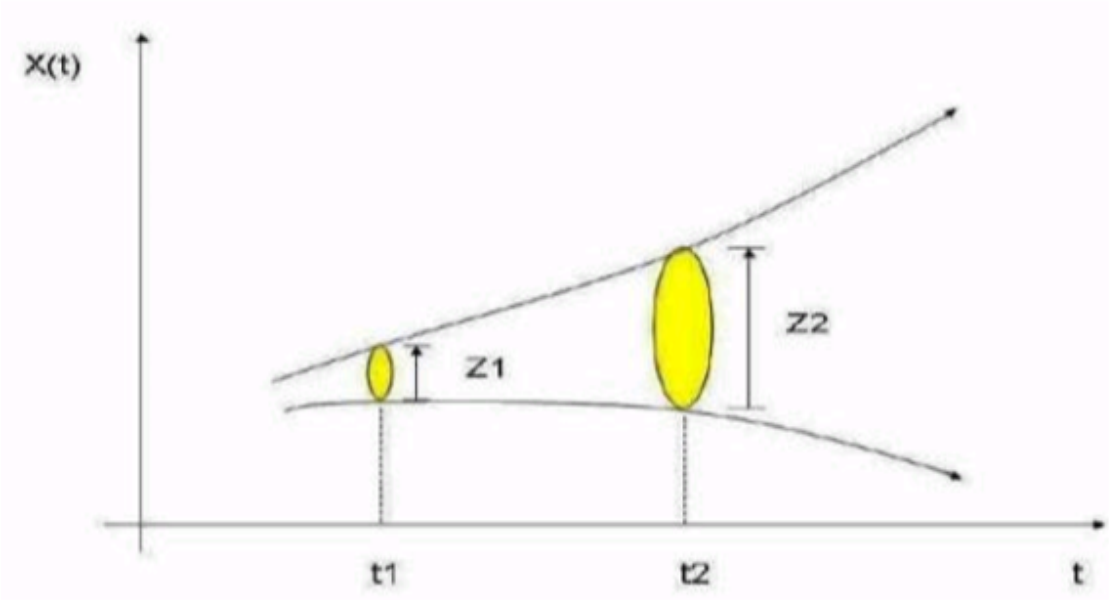
$$\dot{\varepsilon}(t) \approx J_f(X_0) \cdot \varepsilon(t). \quad (2.9)$$

وهذا يعني أن النظام (2.6) أصبح خطياً .

6.2 أسس ليابونوف

تعريف 1.6.2

من الصعب فهم التطور الفوضوي لأن تباعد المسارات على الجاذب يكون سريعًا. ولهذا السبب نحاول قدر الإمكان، قياس أو تقدير سرعة التباعد أو التقارب. يتم تحديد هذه السرعة من خلال أس ليابونوف الذي يميز معدل فصل مسارين قريبين جدًا (راجع الشكل التالي):



لتكن $f : \mathbb{R} \to \mathbb{R}$ دالة من الصنف C^1 . ولتكن x_0 نقطة من $\mathbb{R}$ ، نقوم بتعريف أس ليابونوف $\lambda(x_o)$ على النحو التالي:

$$\lambda(x_0) = \lim_{n\to\infty} \sup \frac{1}{n} \log\left(\left|(f^n)'(x_0)\right|\right) = \lim_{n\to\infty} \sup \frac{1}{n} \sum_{j=0}^{n-1} \log\left(\left|f'(x_j)\right|\right)$$

مع $x_j = f^j(x_o)$

وبالتالي فإن المسارين في مستوى الطور المنفصلين في البداية بمعدل Z_1 ، يتباعدان بعد فترة زمنية $\Delta t = t_2 - t_1$ نحو Z_2 ، بحيث:

$$|Z_2| \approx e^{\lambda \Delta t} |Z_1|$$

حيث λ هو أس ليابونوف.

1.6.2 رقم ليابونوف

تعريف 2.6.2

يستخدم رقم ليابونوف لقياس معدل انفصال النقاط القريبة جدًا بشكل أفضل، حيث أن أس ليابونوف هو اللوغاريتم الطبيعي لرقم ليابونوف، وهذا يعني أن المسارات التي تحيط بالنقطة الثابتة سوف تنفصل عن النقطة في المتوسط عددًا معينًا من المرات في كل تكرار .

نفترض أن الحالة $F_y(x_o)$ هي النقطة التي يتقارب عندها المسار ذو الشرط الأولي إلى بعد I وحدات

زمنية، ولنفترض أن $\dot{x} = f(x_o)$ عبارة عن نظام من المعادلات التفاضلية ذات $x = (x_1, x_2, ..., x_n)$ حالة.

2.6.2 الطريقة الأولى لليابونوف (الطريقة غير المباشرة)

تعتمد هذه الطريقة على إختبار خطية النظام (2.6) بجوار نقطة التوازن X_0 . وبشكل أدق، نقوم بتحليل القيم الذاتية λ للمصفوفة جاكوبي المحسوبة عند نقطة التوازن. واستقرارية X_0 تعطى كالتالي:

نظرية 1.6.2

إذا كانت $(\lambda_k)_{k=1...n}$ هي القيم الذاتية للمصفوفة $Jf(X_0)$، فإن:

1. $\exists k \in \{1, \dots, n\}, \quad \mathrm{Re}(\lambda_k) > 0 \Leftarrow$ فإن نقطة التوازن X_0 غير مستقرة.
2. $\forall k \in \{1, \dots, n\}, \quad \mathrm{Re}(\lambda_k) < 0 \Leftarrow$ فإن نقطة التوازن مستقرة أسّيًا.[3]

ملاحظة

هذه الطريقة لا تسمح بدراسة الاستقرارية إلا جزئيًا، لأنها لا تقدم نتيجة حاسمة إذا كانت بعض القيم الذاتية ذات جزء حقيقي معدوم.

3.6.2 الطريقة الثانية لليابونوف (الطريقة المباشرة)

تُختصر هذه الطريقة في النظرية التالية:

نظرية 2.6.2

لتكن X_0 نقطة توازن للنظام (2.6)، ولتكن $V : D \to \mathbb{R}$ دالة (تُعرف بدالة ليابونوف) من الصنف C^1 معرفة بجوار X_0 بحيث:

1. إذا كان $X \neq X_0$ فإن: $V(X_0) = 0$ و $V(X) > V(X_0)$.
2. $\dot{V}(X) \leq 0 \Rightarrow X_0$ مستقر $, \forall X \neq X_0$
3. $\dot{V}(X) < 0 \Rightarrow X_0$ مستقر بانتظام بمعنى ليابونوف $\forall X \neq X_0$ [3]

مثال: ★

ليكن النظام التالي:

$$(P):\begin{cases}\dot{x}=-x-xy^2,\\ \dot{y}=-y+3yx^2,\end{cases}$$

النظام لديه نقطة توازن في $O(0,0)$، لتكن الدالة التالية:

$$V(x,y)=3x^2+y^2$$

نلاحظ أن: $V(x,y)>0 \quad ;\forall(x,y)\neq(0,0)$ و $V(0,0)=0$ نحسب مشتقة ليابونوف:

$$\begin{aligned}\frac{dV}{dt}&=6x\cdot\dot{x}+2y\cdot\dot{y}\\&=6x\left(-x-xy^2\right)+2y\left(-y+3yx^2\right)\\&=-6x^2-2y^2.\end{aligned}$$

إذاً: $\frac{dV}{dt}<0 \quad ,\forall(x,y)\neq(0,0)$ وبالتالي تكون مستقرة بانتظام.

تعريف 3.6.2 التشعب

التشعب هو تغيير في نقاط التوازن، أو المدارات الدورية، أو في خصائص الاستقرار لنظام غير خطي، عندما يتغير معامل في النظام. يُطلق على هذا المعامل اسم معامل التشعب، والقيم التي يحدث عندها تغيير نوعي في سلوك النظام تُسمى نقاط التشعب.

تعريف 4.6.2 مخطط التشعب

مخطط التشعب هو تمثيل لنقاط التوازن كدالة لمعامل التشعب.
التشعب هو تغيير جذري في سلوك النظام المدروس، ويحدث ذلك غالبًا عند نقاط التوازن. عندما يؤدي تغير في معامل معين إلى تغير في استقرارية النظام، فإن هذا يُعرف بظاهرة التشعب.
هناك أربع أنواع من التشعبات ذات البُعد المشترك :

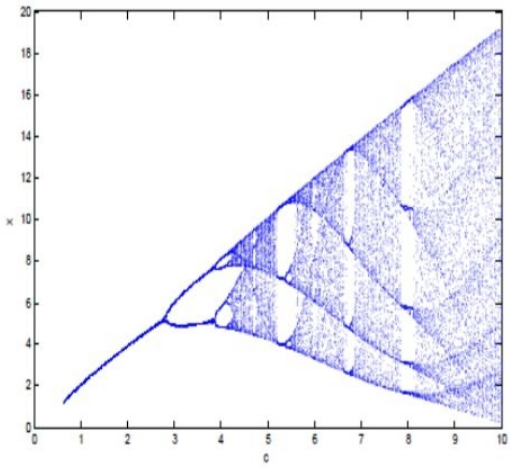
1. التشعب العقدة-السرج (nœud-col) .
2. التشعب التبادلي (transcritique) .
3. التشعب الشوكي (fourche) .
4. تشعب هوبف (Hopf) . .

مثال:

لنأخذ نظام روسلر (Rossler-system) التالي:

$$\begin{cases} \dot{x} = -y - z \\ \dot{y} = x + ay \\ \dot{z} = b + z(x - c) \end{cases}$$

حيث أن a، b، وc هي ثوابت (معاملات تشعب). هذا النظام يشبه نظام لورنز، (Lorenz) وقد تم اقتراحه من قبل العالم الكيميائي الحيوي الألماني أوتو روسلر (Otto-Rössler) في عام 1976. وهو مشتق من معادلات نافييه-ستوكس، (Navier-Stokes) وبالتالي فهو مرتبط بدراسة تدفق الموائع.



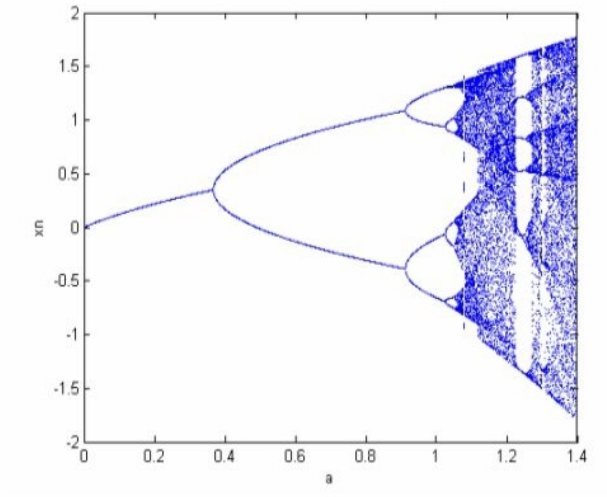
شكل 1.2: مخطط التشعب لنظام روسلر

مثال:

مخطط التشعب لنظام هينون (Hénon-system) :

هو نظام ديناميكي ثنائي الأبعاد يعرف بمعادلته حيث a وb ثوابت:

$$\begin{cases} x_{k+1} = a - x_k^2 + by_k, \quad k = 0, 1, 2, \ldots \\ y_{k+1} = x_k. \end{cases}$$



شكل 2.2: مخطط التشعب لنظام هينون

7.2 الفوضى

لفترة طويلة، كانت الفوضى مرادفة للاضطراب والارتباك. لقد عارضت نظرية الفوضى النظام وكان لابد من تجنبها، وقد تميزت العلوم بالحتمية والقدرة على التنبؤ والعكس. وكان عالم الرياضيات **هنري بوانكاريه Henri Poincaré** من أوائل من لُمحوا لنظرية الفوضى فقد اكتشف مفهوم الحساسية للظُروف الأولية من خلال مشكلة تفاعل ثلاثة أجرام سماوية.

يُعرّف مصطلح "الفوضى" حالة معينة لنظام لا يتكرر سلوكه أبدًا، وهو ما يتميز بالحساسية للظروف الأولية وعدم القدرة على التنبؤ به على المدى الطويل. ومنذ ذلك الحين، بدأ العديد من الباحثين من مختلف التخصصات في الاهتمام بهذا النوع من السلوك.

وهكذا، في هذا الفصل سوف نركز على الأنظمة الديناميكية الفوضوية استناداً إلى المفاهيم الأساسية للأنظمة الديناميكية مثل مفاهيم الجاذبات الغريبة والتشعب.

8.2 النظام الفوضوي

تعريف 1.8.2

النظام الفوضوي هو النظام الذي يكون في حالاته مسارات فوضوية حيث يوجد لدينا نقطتان أوليتان (شروط أولية) مرتبطتان مع بعضهما البعض في البداية وتنفصل مع مرور الوقت، ولا تصلان أبدًا إلى مسار أو مدار مشترك بينهما.

9.2 خصائص النظام الفوضوي

الخصائص:

توجد مجموعة من الخصائص التي تُميّز السلوك الفوضوي والتي تُعتبر معايير رياضية تُستخدم لتحديد ما إذا كان نظام ما فوضويًا. من بين أهم هذه الخصائص نجد:

اللاخطية: النظام الفوضوي يتسم بكونه غير خطّي، أي أن العلاقة بين المتغيّرات ليست بسيطة ولا تتبع تناسبًا مباشرًا. هذا النوع من الأنظمة يصعب التنبؤ بتصرفاته لأنه لا يخضع لقواعد رياضية خطية تقليدية.

اللادورية: النظام الفوضوي لا يُعيد نفس السلوك أو المسار بمرور الوقت. يعني ذلك أن الحركات أو المدارات التي يمرّ بها لا تتكرر، وبالتالي فهي ليست دورية.

الحساسية تجاه الشروط الابتدائية: من أهم خصائص الفوضى أن تغيّرًا بسيطًا جدًا في الحالة الابتدائية للنظام يمكن أن يؤدي إلى نتائج مختلفة تمامًا على المدى البعيد. هذه الظاهرة عُرفت لأول مرة على يد الرياضي "بوانكاريه"، ثم أُعيد اكتشافها سنة 1963 من طرف "لورينز" خلال بحوثه في علم المناخ. هذا التغيّر الحاد في النتائج رغم صغر التغيير في المعطيات الأولية هو ما يجعل التنبؤ بسلوك الأنظمة الفوضوية أمرًا معقدًا.

الحتمية: النظام الفوضوي رغم مظهره العشوائي، إلا أنه محدَّد ويتطوّر وفق قوانين دقيقة ومعادلات رياضية، سواء كانت تفاضلية أو تفاضلية تفريقية. يعني ذلك أن سلوكه ليس عشوائيًا بالكامل، بل تحكمه معادلات، لكنه يتفاعل مع الشروط الابتدائية بطريقة تجعل مخرجاته غير قابلة للتوقع بسهولة.

الجاذب الغريب (أو الجاذب الشاذ): هذا المفهوم يُشير إلى شكل هندسي معقد يُميز تطور النظام الفوضوي في الفضاء الطوري. لا يوجد تعريف دقيق أو موحَّد للجاذب الغريب في الأدبيات، لكن يُعتبر من العلامات الدالة على الفوضى في الأنظمة الديناميكية.

العشوائية: إن الأنظمة الفوضوية تتصرف، في الواقع، بطرق قد تبدو عشوائية. يأتي هذا الجانب العشوائي من الفوضى من حقيقة أننا غير قادرين على تقديم وصف رياضي للحركة، ولكن هذا السلوك في الواقع موصوف بمعادلات غير خطية حتمية تمامًا.

1.9.2 تطبيقات الفوضى

تطبيقات الفوضى	
التطبيق	الوصف
تحكم	التحكم في السلوك غير المنتظم في الدوائر والأنظمة.
تزامن	الاتصالات الآمنة، التشفير الراديو.
معالجة المعلومات	ترميز، فك ترميز، وتخزين المعلومات في أنظمة فوضوية، مثل عناصر الذاكرة والدوائر.
تنبؤ قصير الأجل	الأمراض المعدية، درجة الحرارة، الاقتصاد.

جدول 1.2: جدول يوضح تطبيقات الفوضى

10.2 العلاقة بين التشفير والفوضى

تعريف 1.10.2

توفر تقنيات التشفير المبنية على الفوضى مزيجًا جيدًا من السرعة والأمان العالي والتعقيد وقوة الحوسبة، وما إلى ذلك. العديد من الخصائص تجعل الأنظمة الفوضوية مرشحة وجذابة لأمن الاتصالات. يمكننا أن نذكر أمور أخرى من بينها أن المسارات لا تمر أبدًا عبر نفس الحالة، والجانب العشوائي، تطبيق بسيط نسبيًا للأنظمة الفوضوية. بالإضافة إلى ذلك، منذ التسعينيات، لاحظ العديد من الباحثين أن هناك علاقة مثيرة للاهتمام بين الفوضى والتشفير. في الواقع، العديد من خصائص الأنظمة الفوضوية لها توافقات مماثلة أو متشابهة تقريبًا مع أنظمة التشفير التقليدية. ويوضح الجدول التالي المقارنة بين نظرية الفوضى و التشفير:

الفوضى	التشفير
النظام الفوضوي	نظام شبه فوضوي
تحويل غير خطي	تحويل غير خطي
عدد لانهائي من الحالات	عدد نهائي من الحالات
عدد لا نهائي من التكرارات	عدد محدود من التكرارت
حالة اولية	نص عادي
حالة نهائية	نص مشفر
الشروط الأولية	مفتاح
الحساسية للشروط الأولية	التشويش

جدول 2.2: المقارنة بين نظرية الفوضى و التشفير

تعريف 2.10.2 النقاط الدورية والدورات-p

إذا وُجد $k \geq 1$ بحيث أن $F^k(x) = 0$ ، نقول أن x هي نقطة دورية. ودورة النقطة الدورية هي أصغر عدد صحيح $k \geq 1$ يحقق: $F^k(x) = 0$.

المجموعة $\{x_0, x_1, ..., x_{p-1}\}$ تُشكل دورة من الرتبة p (أو مدار دوري من الرتبة p ، أو $p-$ دورة) إذا كان:

$$\begin{cases} F(x(i)) = 0, & i = 0, 1, ..., p-1 \\ F(x(p-1)) = x(0). \end{cases}$$

بمعنى آخر، كل نقطة في دورة من الرتبة p هي نقطة ثابتة لـ F^p حيث: $F^p(x(i)) = 0$ من أجل $i = 0, 1, ..., p-1$ وليست نقطة ثابتة لـ F^k إذا كان $k < p$.

11.2 أمثلة على الأنظمة الفوضوية

تعريف 1.11.2 نظام لورينز (system Lorenz)

كان إدوارد لورينزي عالم أرصاد جوية هو أول من سلط الضوء على الطبيعة الفوضوية لعلم الأرصاد الجوية. يتم وصف اقتران الغلاف الجوي بالمحيط من خلال نظام معادلات نافير-ستوكس (Navier–Stokes) التفاضلية الجزئية لميكانيكا الموائع. في عام 1963، خطرت للورنز فكرة البحث عن نموذج معادلات لدراسة عدم استقرار رايلي-بينارد (Rayleigh–Bénard) .

لقد لعب هذا النموذج دورا تاريخيا مهما لأن تطوره الزمني يكشف عن سلوك فوضوي. علاوة على ذلك، فقد شكل أول نظام تفاضلي تبديدي مشهور يسمح بملاحظة جاذب غريب لقيم معينة من الإعدادات. في نسخته المعبر عنها في معاملات ومتغيرات مخفضة، يتم كتابة نظام المعادلات التفاضلية الثلاثة المقترنة على النحو التالي:

$$\dot{X} = \sigma(Y - X) \tag{1}$$

$$\dot{Y} = rX - Y - XZ \tag{2}$$

$$\dot{Z} = XY - bZ \tag{3}$$

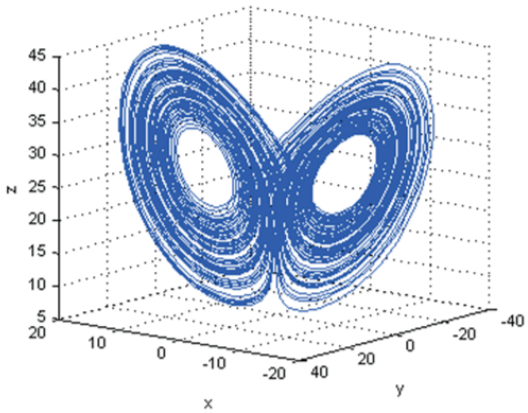
σ أو Pr إلى رقم Prandtl (يساوي 10 في المحاكاة) و $b = 8/3$ و r هو رقم رايلي المختزل. سنقوم بدراسة السلوك والصور الطورية المختلفة التي تم الحصول عليها لقيم مختلفة من إعدادات التحكم.

حساب نقاط التوازن:

وفقا للتعريف تكون النقطة الثابتة على الصورة التالية:

$$\dot{X} = \dot{Y} = \dot{Z} = 0,$$

- النقطة الثابتة التافهة الأولى هي: $P_0 : X = Y = Z = 0, \quad \forall r \geq 0$



شكل 3.2: جاذب نظام لورينز في معلم ثلاثي الأبعاد $\sigma = 10, b = 8/3, r = 28$

من (1) و (3) نجد:

$$X^2 = bZ \Leftrightarrow X = \pm\sqrt{bZ},$$

ومن (1) و (2) نجد:

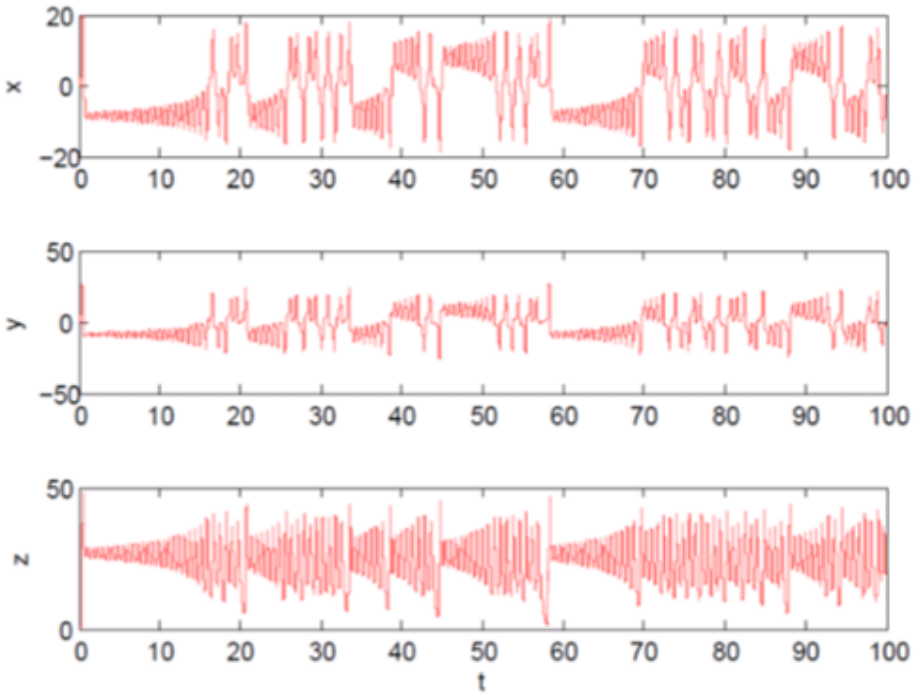
$$-XZ + rZ - Z = 0 \Leftrightarrow Z = r - 1,$$

وبالتالي فإن النقاط الثابتة P_1 و P_2 هي:

$$P_1 = \left(\sqrt{b(r-1)}, \sqrt{b(r-1)}, r-1\right).$$
$$P_2 = \left(-\sqrt{b(r-1)}, -\sqrt{b(r-1)}, r-1\right).$$

إذا كان $r = 0$ فإن $P_0 = P_1 = P_2$ لذا بالنسبة لـ $r \in (0,1)$ فإنه توجد نقطة ثابتة وحيدة فقط هي: P.

أما بالنسبة لـ $r > 1$ فإنه توجد ثلاث نقاط ثابتة P_0, P_1, P_2.



شكل 4.2: السلسلة الزمنية $x(t), y(t), z(t)$ لنظام لورينز $\sigma = 10, b = 8/3, r = 28$

الفصل 3

تزامن الأنظمة الفوضوية

1.3 تزامن الأنظمة الفوضوية 38
2.3 فئات التزامن 40
3.3 أنواع التزامن 40
4.3 التزامن باستخدام طريقة التحكم المستمر 43
5.3 مبدأ التزامن المطابق 43
6.3 التزامن المعمم (GS Generalized-Synchronization) . 47

يعود التزامن إلى القرن السابع عشر، وهو يصف تطور نظامين يتصرفان بالطريقة نفسها وفي الوقت نفسه. في الأدب العلمي، تم اقتراح عدة مفاهيم للتزامن الفوضوي في البداية، مع عمل **فوجيساكا (Fujisaka)** و**يامادا (Yamada)** اللذان استخدما نهجًا محليًا للتزامن الفوضوي. بعد ذلك، طور **أفريموفيتش (Afraimovich)** وآخرون المفاهيم المهمة المرتبطة بالتزامن الفوضوي، ثم عرفا **بيكورا وكارول (Carroll et Pecora)** التزامن الفوضوي باسم التزامن المتماثل (المتطابق)، والذي تم تطويره بناءً على دوائر فوضوية مقترنة، حيث يكون أحدهما مرسلًا والآخر مستقبلًا.

إن مجالات استخدام التزامن واسعة، فهي موجودة في مختلف العلوم، وخاصة في مجال الاتصالات، حيث تعتبر مفتاحًا مهمًا لنجاح الإرسال. إذ يتعلق استخدام الأنظمة الفوضوية في الإرسال الآمن بإخفاء الرسالة المشفرة داخل إشارة فوضوية وعند الاستقبال، يتم تنفيذ العملية العكسية وهي استخراج الرسالة ثم فك تشفيرها.

1.3 تزامن الأنظمة الفوضوية

يهدف هذا الفصل إلى تقديم تعريف التزامن، أنواعه وطرقه.

1.1.3 تعريف التزامن

تعريف 1.1.3 موسوعة لاروس (Encyclopédie Larousse)

التزامن هو كلمة يونانية تتكون من جزأين: "Syn" تعني معًا، و "Chrono" تعني الزمن. وهو فعل المزامنة لخلق تزامن بين عدة عمليات بناءً على الزمن.

تعريف 2.1.3 التعريف العام

التزامن هو آلية تهدف إلى الحفاظ على تطوّر منظم — سواء دوري أو فوضوي — بين نظامين ديناميكيين. ويُقصد بتزامن نظامين فوضويين أن كلاً منهما يتبع سلوك الآخر بمرور الزمن. يستند هذا المفهوم إلى خاصية جوهرية في الأنظمة الفوضوية، وهي أنها أنظمة حتمية تمتلك على الأقل قيمة موجبة لـ أسس ليابونوف، ما يجعلها ذات حساسية عالية للظروف الابتدائية، وبالتالي غير مستقرة.

عندما يتم ربط نظامين من خلال آلية اقتران — أي عبر تبادل للطاقة أو الإشارة بينهما — يصبح من الممكن تحقيق التزامن بينهما. وبشكل أدق، تُعتبر إشارتان فوضويتان متزامنتين إذا اقترب الفرق بينهما تقاربيًا نحو الصفر عندما يقترب الزمن من اللانهاية.

تعريف 3.1.3 التعريف الرياضي للتزامن

بعد عدة محاولات لتعريف الحركة المتزامنة، تمكن الباحثان "براون" و"كوكاريف" (**et Brown Kocarev**) من تقديم تعريف رياضي للتزامن. لبناء هذا التعريف، افترضا أن النظام الديناميكي العام ذو البعد المحدود والحتمي، يمكن تقسيمه إلى نظامين فرعيين:

$$\begin{cases} \dfrac{dX}{dt} = f_1(X,Y,t)), \\ \dfrac{dY}{dt} = f_2(Y,X,t). \end{cases} \qquad (3.1)$$

حيث $X \in \mathbb{R}^n$ و $Y \in \mathbb{R}^m$ هما شعاعان قد يكونا ذو بعدين مختلفين. ليكن $\varphi(\omega_0)$ مسار للنظام العام المعطى بالجملة (3.1) مع الشرط الإبتدائي: $\omega_0 = [X_0, Y_0] \in \mathbb{R}^n \times \mathbb{R}^m$.

بالنسبة لكل نظام فرعي، نكوّن مسارًا $\varphi_X(\omega_0)$ و $\varphi_Y(\omega_0)$ (حيث ω_0 يمثل الشرط الإبتدائي

المعطى). نرمز بـ $\mathcal{X}$ إلى فضاء جميع مسارات النظام الفرعي الأول، وبـ ζ إلى فضاء جميع مسارات النظام الفرعي الثاني، ونعتبر الدالتين $g_X : \mathcal{X} \times \mathbb{R} \to \mathbb{R}^d$ و $g_Y : \zeta \times \mathbb{R} \to \mathbb{R}^d$، غير معدومتين، حيث يمثل $\mathbb{R}$ فضاء الزمن. نقول إن الدالتين g_X و g_Y هما خاصيتين للنظامين الفرعيين المعرفتين بالجملة (3.1) على التوالي. أخيرًا لتعريف حالة التزامن، يشترط "براون" و"كوكاريف" وجود دالة: $h(g_X, g_Y) : \mathbb{R}^d \times \mathbb{R}^d \to \mathbb{R}^d$ بحيث $\|h\| = 0$ أو $\|h\| \to 0$. نقول إن الدالة h التي لا تتعلق بالزمن تقارن بين الدالتين المقاستين على النظامين الفرعيين، وتتقارب القياسات مع الزمن إذا وفقط إذا كان $h(g_X, g_Y) = 0$.

تعريف 4.1.3 براون و كوكاريف

يُقال إن النظامين الفرعيين في الجملة (3.1) متزامنان على المسار $\varphi(\omega_0)$، بالنسبة إلى الدالتين g_X و g_Y، إذا وجدت لحظة زمنية مستقلة عن التطبيق h بحيث $\|h(g_X, g_Y)\| = 0$. إن اختيار الدوال g_X و g_Y و h، يمكننا من تحديد نوع التزامن، مما يعني وجود أنواع مختلفة من التزامن التي تدخل ضمن نفس الإطار الرياضي الموحد.

نظرية 1.1.3

لكي يكون النظام المتحكم (المرسل)والنظام التابع (المرسل إليه) متزامنين، فإن الشرط اللازم والكافي هو أن تكون جميع أسس ليابونوف للنظام التابع (المسماة أسس ليابونوف الشرطية) سالبة.

$$\forall i \quad \lambda_i^{cond} < 0.$$

2.1.3 معيار راوث-هورفيتز (Routh-Hurwitz)

تعريف 5.1.3

معيار راوث-هورفيتز هو أداة رياضية حاسمة تُستخدم للتأكد من استقرار النظام دون الحاجة لحساب جذور المعادلة المميزة فعلياً. يعتمد على فحص إشارات معاملات متعددة الحدود التي تصف ديناميكيات النظام.

بشكل مبسط:

* الشروط الأولية: يجب أن تكون جميع معاملات المعادلة المميزة موجودة ولها نفس الإشارة (عادةً موجبة).

* بناء المصفوفة: تُبنى "مصفوفة راوث" باستخدام هذه المعاملات.

* شرط الاستقرار: يكون النظام مستقراً إذا كانت جميع العناصر في العمود الأول من هذه المصفوفة لها نفس الإشارة. إذا تغيرت الإشارة، فهذا يعني عدم الاستقرار.

ربطه بسياق الأنظمة الفوضوية والمزامنة:

في سياق المزامنة بين الأنظمة الفوضوية وتصميم المُزامِن (الذي يستخدم صيغة مثل: $u = -ax + (1+c)y$) يُستخدم معيار راوث-هورفيتز لضمان استقرار النظام المركب الناتج عن ربط النظام الفوضوي بالمزامن. عند تصميم هذا الأخير، يتم اختيار معاملات التحكم بحيث تحقق المعادلة المميزة شروط الاستقرار، مما يضمن تزامنًا مستقرًا من خلال اضمحلال خطأ التزامن تدريجيًا، نتيجة وقوع جميع الأقطاب في النصف الأيسر من المستوى المركب.

2.3 فئات التزامن

توجد فئتان رئيسيتان للتزامن بناءً على طريقة تبادل الطاقة بين النظامين الفوضويين: التزامن بالاقتران أحادي الاتجاه والتزامن بالاقتران ثنائي الاتجاه.

1.2.3 التزامن بالاقتران أحادي الاتجاه

النظام المتحكم (المرسل): هو نظام مستقل لا يتأثر بالنظام الآخر.

النظام التابع (المستقبل): هو نظام يعتمد في تطوره على النظام المتحكم (المرسل).

في التزامن بالاقتران أحادي الاتجاه، يتم نقل الطاقة من نظام إلى آخر عبر عنصر يعمل في اتجاه واحد فقط. وبالتالي، يوجد نظام متحكم واحد فقط (المرسل) ونظام تابع واحد فقط (المستقبل). مثال على ذلك استخدام دائرة كهربائية تتبعية.

2.2.3 التزامن بالاقتران ثنائي الاتجاه

في الاقتران ثنائي الاتجاه، تنتقل الطاقة بين النظامين في كلا الاتجاهين، مما يعني أن كل نظام يمكن أن يلعب دور النظام الرئيسي والنظام التابع في نفس الوقت. يمكن تحقيق ذلك باستخدام عناصر بسيطة مثل المقاومة الكهربائية.

3.3 أنواع التزامن

في المراجع العلمية، تم اقتراح أنواع مختلفة من التزامن، منها التزامن المتماثل، والتزامن المعمم، وتزامن الطور...إلخ.

ملاحظة ★

العمل المقدم في هذه المذكرة يركز على تزامنين فقط هما المتماثل والمعمم.

1.3.3 التزامن المتماثل

يُتحقّق التزامن المتماثل (المعروف أيضًا باسم التزامن الكامل) نتيجة تأثير قوى الاقتران أحادي الاتجاه بين الأنظمة الديناميكية، سواء كانت ذاتية أو غير ذاتية. وتكمن أهميته في كونه يمثل حالة خاصة تشمل أنواعًا مختلفة من التزامن، مثل التزامن المعمم، وتزامن الطور، والتزامن المتأخر. يعتمد هذا النوع من التزامن على طبيعة الاقتران بين نظامين أو أكثر، فإذا كانت الأنظمة متماثلة من حيث البنية والديناميكيات، فإننا نتحدث عن تزامن متماثل، أما إذا كانت مختلفة، فيُصنَّف التزامن ضمن إطار التزامن المعمم.

تعريف 1.3.3

لنفترض وجود نظامين ديناميكيين متماثلين مرتبطين باقتران أحادي الاتجاه، ويمثلان بالمعادلتين التاليتين:

$$\dot{X} = f(X,t), \quad (3.2)$$
$$\dot{Y} = g(X,Y,t). \quad (3.3)$$

نقول إن هناك تزامنًا متماثلًا بين هذين النظامين إذا:

$$\lim_{t\to\infty} |Y(t) - X(t)| = 0. \quad (3.4)$$

لجميع الشروط الإبتدائية $X(o)$، $Y(o)$ للنظامين (3.2)و (3.3).

ملاحظة ★

يبقى هذا التعريف صالحاً عند تطبيق طريقة كارول وبيكورا، بشرط تحقق العلاقة التالية:

$$\lim_{t\to\infty} |Y(t) - X_2(t)| = 0. \quad (3.5)$$

حيث $X_2(t)$ شعاع فرعي من $X(t)$، وهو ما يُمثّل شرط التزامن كما ورد في المعادلة (3.4) بصيغة مكافئة.

بناءً على هذا التعريف، يمكن استنتاج أن دراسة تزامن الأنظمة يؤدي إلى دراسة الاستقرار بجوار الأصل لنظام جديد يسمى "نظام الخطأ"، حيث يمثل هذا الأخير الفرق بين النظام المرسل والنظام المستقبل. لتحديد ما إذا كان الفرق يتجه نحو الصفر بشكل أسي أو لا، ومن أجل هذا نفترض أن الفرق الصغير بين النظامين يعطى بالمعادلة:

$$e = Y - X.$$

حيث يُمثّل $e(t)$ شعاع الخطأ الناتج عن الفرق بين مخرجات النظامين. ويتطوّر هذا المتجه مع الزمن وفقًا للمعادلة

$$\frac{de}{dt} = g(X,Y) - f(X). \quad (3.6)$$

لدراسة استقرار هذا النظام الديناميكي، نتبع الخطوات التالية:

★ تحويل النظام (3.6) إلى نظام خطي في جوار نقاط توازنه (من الواضح أن نقطة التوازن الوحيدة هي $X = Y$)إذن:

$$\frac{de}{dt} = J(X) \cdot e.$$

حيث $J(X)$ هي المصفوفة اليعقوبية المُعرفة كالتالي:

$$J(X) = \left[\frac{\partial g(X,Y)}{\partial y}\right]_{Y=X}. \quad (3.7)$$

★ تطبيق الطريقة الثانية لليابونوف لتحليل الاستقرار، وذلك باختيار دالة ليابونوف التي تحقق شروط الاستقرار.

★ حساب أسس ليابونوف لنظام المستقبل لضمان استقراره التقاربي.

4.3 التزامن باستخدام طريقة التحكم المستمر

لنفرض نظامين فوضويين ممثلين بالمعادلتين:

$$\begin{cases} \dot{X} = f(X), \\ \dot{Y} = f(Y) + M_{n\times n}(Y - X). \end{cases} \qquad (3.8)$$

حيث:

- $X = (x_1, x_2, \dots, x_n)$ و $Y = (y_1, y_2, \dots, y_n)$ أشعة الحالة.
- f دالة غير خطية.
- $M_{n\times n}$ مصفوفة قطرية ثابتة من الرتبة n.

وبما أن f غير خطية، يمكن إعادة صياغة النظام (3.8) بالشكل:

$$\begin{cases} \dot{X} = AX + \phi(X), \\ \dot{Y} = AY + \phi(Y) + M_{n\times n}(Y - X). \end{cases}$$

حيث A تمثل مصفوفة ثابتة وϕ تمثل الجزء غير الخطي لكل نظام.
ديناميكية نظام الخطأ تعطى وفق العبارة التالية:

$$\dot{e} = A.e + \phi(Y) - \phi(X) + M_{n\times n}.e. \qquad (3.9)$$

إنطلاقا من (3.9) يمكن دراسة استقرارية نظام الخطأ بجوار نقطة التوازن.

5.3 مبدأ التزامن المطابق

نعتبر النظامين الفوضويين المطابقين والمعرّفين بالمعادلتين التاليتين:

$$\dot{X} = A.X + \phi(X). \qquad (3.10)$$

$$\dot{Y} = A.Y + \phi(Y) + M_{n\times n}(Y - X). \qquad (3.11)$$

يرتبط هذان النظامان من خلال اقتران أحادي الاتجاه، حيث X و Y هما متغيرا النظامين المتحكم (3.10) والتابع (3.11) على التوالي.

$$M_{n\times n} = \begin{pmatrix} p_1 & \cdots & \cdots \\ \vdots & \ddots & \vdots \\ \vdots & \cdots & p_n \end{pmatrix}.$$

حيث $M_{n\times n}$ هي مصفوفة قطرية، A مصفوفة مربعة من الرتبة n وϕ دالة مستمرة غير خطية من الرتبة n تحقق شرط Lipschitz التالي:

$$\|\phi(X) - \phi(Y)\| \leq \rho\|X - Y\|. \quad (3.12)$$

ρ هو ثابت Lipschitz و$\|\cdot\|$ هو النظيم الإقليدي (المعيار الإقليدي). وبالتالي لدينا النظرية التالية:

نظرية 1.5.3

لتكن E مصفوفة الوحدة من الرتبة $n \times n$ و$\{\lambda_i\}_{i=1}^n$ القيم الذاتية للمصفوفة المتناظرة:

$$\frac{(A + M_{n\times n}) + (A + M_{n\times n})^T}{2} + \rho E.$$

إذا كان $\max\{\lambda_i\}_{i=1}^n < 0$، فإن النظام المرسل (3.10) والنظام المستقبل (3.11) يكونان متزامنين بمعنى أن نظام الخطأ يتجه نحو الصفر بشكل أسي.

البرهـــــان:

نعتبر نظام الخطأ التالي:

$$e = Y - X,$$

توصف ديناميكية هذا النظام بالمعادلة:

$$\dot{e} = (A + M_{n\times n})e + \phi(Y) - \phi(X),$$

بما أن $\{\lambda_i\}_{i=1}^n$ هي القيم الذاتية للمصفوفة المتناظرة:

$$\frac{(A + M_{n\times n}) + (A + M_{n\times n})^T}{2} + \rho E,$$

فإن هذه المصفوفة مشابهة للمصفوفة القطرية:

$$\Lambda = \begin{pmatrix} \lambda_1 & \cdots & \cdots \\ \vdots & \ddots & \vdots \\ \vdots & \cdots & \lambda_n \end{pmatrix} = \mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n).$$

بواسطة مصفوفة متعامدة U تحقق:

$$U^T\left[\frac{(A+M_{n\times n})+(A+M_{n\times n})^T}{2}+\rho E\right]U=\Lambda,$$

لنعتبر دالة ليابونوف $V(e)$ لنظام الخطأ المعرفة بالعلاقة: $V(e)=\frac{1}{2}\|e\|^2$ من الواضح أن $V(e)>0$.
الآن نحسب مشتقة $\dot{V}(e)$:

$$\begin{aligned}\dot{V}(e)&=\frac{1}{2}\left(\dot{e}^Te+e^T\dot{e}\right)\\&=\frac{1}{2}\left[((A+M_{n\times n})e+\phi(X)-\phi(Y))^Te+e^T((A+M_{n\times n})e+\phi(X)-\phi(Y))\right]\\&=\frac{1}{2}\left[e^T(A+M_{n\times n})^Te+e^T(A+M_{n\times n})e+(\phi(X)-\phi(Y))^Te+e^T(\phi(X)-\phi(Y))\right],\end{aligned}$$

باستخدام شرط ليبشيتز $\|\phi(X)-\phi(Y)\|\leq\rho\|e\|$، نحصل على:

$$\begin{aligned}\dot{V}(e)&\leq e^T\left[\frac{(A+M_{n\times n})+(A+M_{n\times n})^T}{2}+\rho E\right]e\\&\leq e^TU\Lambda U^Te=\left(U^Te\right)^T\Lambda\left(U^Te\right)\\&\leq\max\{\lambda_i\}_{i=1}^n\left(U^Te\right)^T\left(U^Te\right)\\&\leq 0.\qquad e\neq 0\end{aligned}$$

وبالتالي:

$$t\to\infty\Rightarrow V(e)\to 0.$$

مما يعني أن $e\to 0$ عندما $t\to\infty$.

1.5.3 التزامن بطريقة كارول وبيكورا

هذه الطريقة تم اقتراحها من قبل الباحثين بيكورا وكارول عام 1990، حيث أظهرا أن نظامين فوضويين متماثلين يمكن أن يتزامنا تحت شروط معينة. تتميز هذه الطريقة بأنها توفر حلاً بسيطاً وفعالاً لمشكلة تزامن الأنظمة. كما تسمح للنظام التابع (المستقبل) بأن يكرر بدقة كبيرة حالة النظام الرئيسي (المرسل). تتمحور فكرة هذه الطريقة حول تقسيم النظام الأصلي إلى نظامين فرعيين. يمكن تنفيذ هذه العملية من خلال إعادة ترتيب متغيرات الحالة دون التقيد بترتيب معين..

لنفترض نظاماً ديناميكياً ذاتياً زمنياً مستمراً ذو البعد n:

$$\dot{X} = f\left(X\left(t\right)\right), \qquad (3.13)$$

حيث:

$$X = \left[x_1, \ldots, x_n\right]^T,$$

هو شعاع الحالة.

يتم تقسيم النظام الأصلي إلى نظامين فرعيين S_1 و S_2 مع إعادة ترتيب متغيرات الحالة دون التقيد بترتيب معين:

$$\begin{cases} S_1 : \dot{X}_1 = F_1\left(X_1, X_2\right), \\ S_2 : \dot{X}_2 = F_2\left(X_1, X_2\right). \end{cases} \qquad (3.14)$$

حيث:

$$X_1 = \left[x_1, \ldots, x_m\right]^T,$$
$$X_2 = \left[x_{m+1}, \ldots, x_n\right]^T,$$
$$F(X) = \left[F_1(X); F_2(X)\right],$$

الآن نعتبر نظاماً فرعياً آخر S_2' يتميز بديناميكية مماثلة لـ F_2، مع شعاع الحالة $\hat{X}_2$:

$$S_2' : \dot{\hat{X}}_2 = F_2\left(X_1, \hat{X}_2\right). \qquad (3.15)$$

أثبت بيكورا وكارول أن الشرط الضروري والكافي لتحقيق التزامن بين النظام الأصلي والنظام الفرعي S_2' هو أن يكون هذا الأخير مستقراً، أي أن تكون جميع أسس ليابونوف **سالبة** . وبالتالي يتم تحقيق تزامن مثالي حيث تصبح المسارات متقاربة:

$$\lim_{t \to \infty} \left\| \hat{X}_2\left(t\right) - X_2\left(t\right) \right\| = 0. \qquad (3.16)$$

6.3 التزامن المعمم (GS Generalized-Synchronization)

يُعد التزامن المعمم امتدادًا طبيعيًا للتزامن المتماثل، ويُطبَّق في حالات الأنظمة الفوضوية تختلف إما في الأبعاد أو في النماذج الديناميكية. يتميّز هذا النوع من التزامن بوجود علاقة وظيفية غير خطية تربط بين حالتي نظامين فوضويين مختلفين.

مقارنةً بالتزامن المتماثل، فإن التزامن المعمم (GS) يُقدّم ديناميكيات أكثر تعقيدًا ومرونة، حيث يمكنه من استيعاب حالات عدم التزامن حتى في ظل اختلاف المعاملات النظامية أو تشوه الإشارات أثناء الإرسال أو التشويش.

ونظرًا لهذه المرونة، فإن مجال تطبيقات GS أوسع نطاقًا، مما يجعله خيارًا مناسبًا في أنظمة الاتصالات المشفرة والأنظمة غير الخطية المعقدة، حيث يصعب تحقيق تزامن متماثل.

تعريف 1.6.3 التزامن المعمم

من أجل تعريف التزامن المعمم لمخطط اقتران باتجاه واحد، نعتبر نظامًا مرسلًا ذاتيًا بمتغيرات ديناميكية x في فضاء الطور X، مقترنًا بنظام مستقبل بمتغيرات ديناميكية y في فضاء الحالة Y. يتم تمثيل النظامين بالمعادلتين:

$$\dot{x} = F(x(t)). \quad (3.17)$$

$$\dot{y} = G(y(t), g, x(t)). \quad (3.18)$$

حيث g ثابت يمثل قوة الاقتران أحادي الاتجاه.

إذا كان $g \neq 0$ ووجد تحويل $\phi : X \to Y$ بحيث يحقق جميع مسارات النظام المرسل والمستقبل، مع الشروط الأولية $x(0)$ و $y(0)$، يحقق العلاقة التالية:

$$\lim_{t\to\infty} \|y(t) - \phi(x(t))\| = 0, \quad \forall x(0), y(0).$$

فإن النظامين (3.17) و (3.18) يكونان متزامنين بشكل معمم بالنسبة لـ ϕ.

ملاحظة ★

يتطلب تعريف التزامن المعمم هذا وجود تحويل ϕ فقط للمسارات الواقعة على الجاذب، دون اشتراط وجوده للمسارات العابرة.

1.6.3 كشف واستقرار التزامن المعمم

للكشف عن التزامن المعمم ودراسة استقراره، تم اقتراح عدة طرق، من بينها الطريقة المعروفة بإسم "النظام المساعد التقريبي":

طريقة النظام المساعد التقريبي:

1. **الأساس النظري:** تقوم فكرة هذه الطريقة على أنه إذا قام نفس النظام المرسل $x(t)$ بتوجيه نظامين مستقبلين متطابقين $y(t)$ و $z(t)$ بشرطين ابتدائيين مختلفين ضمن حوض الجذب، فإن تحليل استقرارية التزامن في الفضاء المركب $X \oplus Y$ (الذي قد يتخذ شكلاً جد معقد $y(t) = \phi(x(t))$) يمكن استبداله بتحليل بسيط لاستقرارية $z(t) = y(t)$ في الفضاء $Z \oplus Y$.

2. **التنفيذ الرياضي:** يُعرّف النظام المساعد بالمعادلة التفاضلية التالية:

$$\dot{z} = G(z(t), g, x(t)). \quad (3.19)$$

حيث يتطابق هذا النظام تمامًا مع النظام المستقبل (3.18) . عندما يتشارك النظام المستقبل (3.18) ونظامه المساعد (3.19) نفس إشارة الإرسال $x(t)$، تصبح حقول الأشعة في فضاء الطور للنظامين متطابقة، مما يضمن تطورهما على جاذبين متماثلين.

3. **نظرية الاستقرار:** يمكن إثبات أن الاستقرار الخطي للمجمع $z(t) = y(t)$ يكافئ الاستقرار الخطي لمجمع الحركات المتزامنة في $X \oplus Y$، والذي تحدده الدالة ϕ.

4. **الخاتمة:** توفر هذه الطريقة إطارًا رياضيًا قويًا لتحليل التزامن المعمم في الأنظمة الفوضوية، مع تجنب التعقيدات الناتجة عن التحليل المباشر للعلاقة $y(t) = \phi(x(t))$.

الفصل 4

تطبيق

1.4 التزامن المطابق لنظام Chen باستخدام طريقة Carroll وPecora 50

تمتلك الأنظمة الفوضوية عدة خصائص مهمة تجعلها ملائمة لأمن الاتصالات، مثل الحتمية، والحساسية لشروط البدء، والمظهر العشوائي، وهي خصائص يمكن ربطها بخصائص التشفير التقليدي مثل التشويش والنشر. ولهذا، فقد اهتم الباحثون بإمكانية استخدام الإشارات الفوضوية في أنظمة نقل البيانات، وخاصةً من أجل نقل كميات كبيرة من المعلومات بشكل آمن. وتكمن فائدة استخدام الإشارات الفوضوية في خاصيتين رئيسيتين من خصائص الفوضى:

1. الإشارة الفوضوية هي إشارة عريضة الطيف، مما يتيح إمكانية نقل إشارات متنوعة ومختلفة بدرجة كبيرة.
2. يتم توليد الإشارة الفوضوية من نظام حتمي، مما يسمح بإعادة توليدها من جديد إذا تم ضبط النظام المستقبل وفقًا لنفس الشروط التي وُلدت فيها، وبالتالي يمكن استعادة المعلومات الأصلية.

1.4 التزامن المطابق لنظام Chen باستخدام طريقة Carroll وPecora

1.1.4 نظام Chen

تم اكتشاف نظام Chen من خلال عملية "التحويل إلى نظام فوضوي" أو ما يسمى "مضاد التحكم" لنظام لورينز المتحكم فيه. أي، انطلاقا من نظام غير فوضوي حاول الباحثون توليد نظام فوضوي باستخدام طريقة ردود فعل الحالة. يُعطى نظام لورينز المتحكم فيه بـ:

$$\begin{cases} \dot{x} = a(y-x), \\ \dot{y} = (c-a)x - xz + cy, \\ \dot{z} = xy - bz, \end{cases} \tag{4.1}$$

حيث a, b, c ثوابت، و u يمثل المتحكم الخطي وفق طريقة ردود فعل الحالة،بالشكل التالي:

$$u = k_1x_1 + k_2y_1 + k_3z_1,$$

مع k_1, k_2, k_3 ثوابت يتم تحديدها. نرغب في أن يصبح النظام (4.1) فوضويًا؛ لذلك يكفي اختيار k_1, k_2, k_3 بحيث يظهر النظام سلوكًا فوضويًا. نقاط التوازن للنظام (4.1) هي: $P_1(0,0,0)$,

$$P_{2,3}\left(\pm\sqrt{b(2c-a)},\ \pm\sqrt{b(2c-a)},\ 2c-a\right),$$

مصفوفة جاكوبيان للنظام (4.1) عند النقطة (x_0, y_0, z_0) تعطى بالصيغة:

$$J_{(x_0;y_0;z_0)} = \begin{pmatrix} -a & a & 0 \\ c+k_1-z_0 & k_2-1 & k_3-x_0 \\ y_0 & x_0 & -b \end{pmatrix},$$

نلاحظ أنه عند نقطة التوازن $P_1(0,0,0)$ تكون مصفوفة جاكوبيان المقابلة لها:

$$J_{(0;0;0)} = \begin{pmatrix} -a & a & 0 \\ c+k_1 & k_2-1 & k_3 \\ 0 & 0 & -b \end{pmatrix},$$

لا يساهم المعامل k_3 في القيم الذاتية، وبالتالي لا يساهم في مُعامِلات بيابونوف، لذا لتبسيط النموذج، اختار Chen أن يكون $k_3 = 0$. ولضمان السلوك الفوضوي، يجب أن تحتوي كل نقطة توازن على الأقل على قيمة ذاتية غير مستقرة واحدة. وباستخدام معايير Routh-Hurwitz، يمكن اختيار

$k_1 = -a$، و $k_2 = 1 + c$ كاختيار بسيط من بين اختيارات أخرى. وبالتالي يصبح قانون التحكم الذي نطبقه للمزامنة هو:

$$u = -ax + (1 + c)y,$$

ويصبح النظام (4.1):

$$\begin{cases} \dot{x} = a(y - x), \\ \dot{y} = (c - a)x - xz + cy, \\ \dot{z} = xy - bz, \end{cases}$$

ويسمى هذا بـ **نظام Chen**

سنقوم بمزامنة نظامين متطابقين من نظام Chen باستخدام طريقة Carroll وPecora، وسندرس كل الحالات الممكنة.

2.1.4 عندما يكون الإشارة المُرسِلة هي x

نفترض أن النظام المرسل يعطى بالشكل التالي:

$$\begin{cases} \dot{x}_1 = a(y_1 - x_1), \\ \dot{y}_1 = (c - a)x_1 - x_1z_1 + cy_1, \\ \dot{z}_1 = x_1y_1 - bz_1, \end{cases}$$

والذي يمكن تفكيكه إلى نظامين فرعيين عبر التعويض:

$$X_1 = (x_1), X_2 = (y_1, z_1),$$

وبالتالي، يكون النظام المرسل في هذه الحالة:

$$\begin{cases} \dot{y}_1 = (c - a)x_1 - x_1z_1 + cy_1, \\ \dot{z}_1 = x_1y_1 - bz_1, \end{cases} \tag{4.2}$$

بينما يكون النظام المستقبل على الشكل:

$$\begin{cases} \dot{y}_2 = (c - a)x_1 - x_1z_2 + cy_2, \\ \dot{z}_2 = x_1y_2 - bz_2, \end{cases} \tag{4.3}$$

نُدخل المتغيرات التالية:

$$\begin{cases} e_y = y_2 - y_1, \\ e_z = z_2 - z_1, \end{cases}$$

وباستخدام النظامين (4.2) و(4.3) نحصل على نظام الخطأ:

$$\begin{cases} \dot{e}_y = ce_y - x_1 e_z, \\ \dot{e}_z = x_1 e_y - be_z, \end{cases} \qquad (4.4)$$

نختار دالة ليابونوف بالشكل:

$$V_1 = \frac{1}{2}({e_y}^2 + {e_z}^2),$$

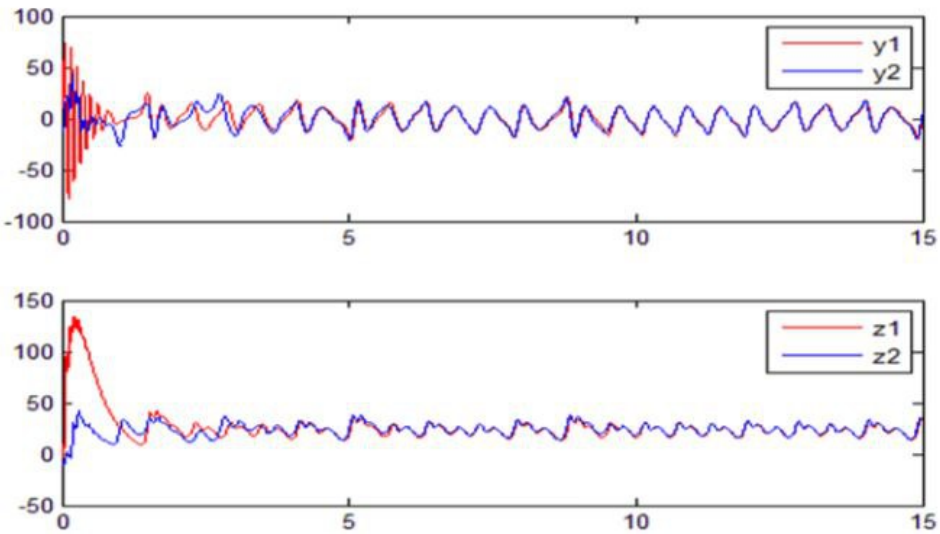
مشتقتها الزمنية هي:

$$\dot{V}_1 = c{e_y}^2 - b{e_z}^2,$$

لكي يكون النظام (4.4) مستقراً أُسّياً في جوار الأصل، يكفي أن:

$$\dot{V}_1 < 0 \Rightarrow e_y < \sqrt{\frac{b}{c}} e_z.$$

محاكاة عددية: من أجل القيم: $(a; b; c) = (35; 3; 28)$,
والقيم الابتدائية: $(x_1; y_1; z_1) = (50; 10; 10)$ $(y_2; z_2) = (-10; -10)$ نحصل على:



شكل 1.4: التزامن المطابق لنظام Chen عندما يكون x هو الإشارة المرسِلة.

3.1.4 عندما تكون فيها الإشارة المُرسِلة هي y

في هذه الحالة، يكوم النظام المرسل على الشكل :

$$\begin{cases} \dot{x}_1 = a(y_1 - x_1), \\ \dot{z}_1 = x_1 y_1 - b z_1, \end{cases} \qquad (4.5)$$

بينما يكون النظام المستقبل كما يلي:

$$\begin{cases} \dot{x}_2 = a(y_2 - x_2), \\ \dot{z}_2 = x_2 y_2 - b z_2, \end{cases} \qquad (4.6)$$

انطلاقا من المعادلتين (4.5) و (4.6) ينتج نظام الخطأ:

$$\begin{cases} \dot{e}_x = -a e_x, \\ \dot{e}_z = y_1 e_x - b e_z, \end{cases}$$

حيث:

$$e_x = x_2 - x_1 ; e_z = z_2 - z_1.$$

دالة ليابونوف المقترحة:

$$V_2 = \frac{1}{2}({e_x}^2 + {e_z}^2),$$

مشتقتها تعطى بـ:

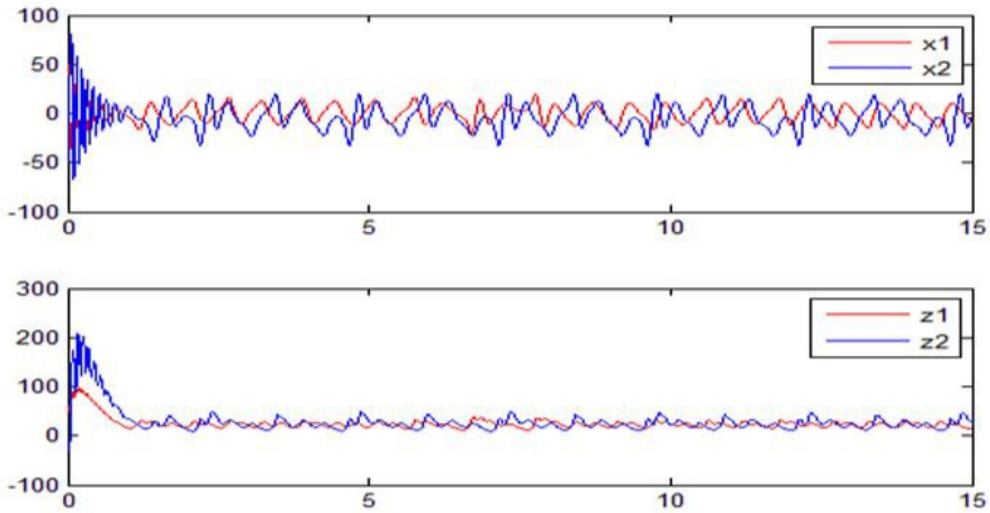
$$\dot{V}_2 = -(a e_x^2 + b e_z^2) + y_1 e_x e_z.$$

لكي يتزامنا النظامان (4.5) و (4.6) ، يكفي أن يكون:

$$y_1 < \frac{a e_x^2 + b e_z^2}{e_x e_z}.$$

محاكاة عددية: من أجل القيم: $(a; b; c) = (35; 3; 28)$

والقيم الابتدائية: $(x_1; y_1; z_1) = (50, 35, 50)$; $(y_2; z_2) = (-50, 29)$ نحصل على:



شكل 2.4: التزامن المطابق لنظام Chen عندما يكون y هو الإشارة المرسِلة.

4.1.4 عندما تكون الإشارة المُرسِلة هي z

في هذه الحالة، يكوم النظام المرسل على الشكل :

$$\begin{cases} \dot{x}_1 = a(y_1 - x_1), \\ \dot{y}_1 = (c-a)x_1 - x_1 z + c y_1, \end{cases} \tag{4.7}$$

بينما يكون النظام المستقبل على الشكل:

$$\begin{cases} \dot{x}_2 = a(y_2 - x_2), \\ \dot{y}_2 = (c-a)x_2 - x_2 z + c y_2, \end{cases} \tag{4.8}$$

انطلاقا من المعادلتين (4.7) و (4.8) ينتج نظام الخطأ:

$$\begin{cases} \dot{e_x} = a(e_y - e_x), \\ \dot{e_y} = (c-a)e_x - e_x z + c e_y, \end{cases}$$

مع: $e_x = x_2 - x_1$ و $e_y = y_2 - y_1$.

دالة ليابونوف المقترحة:

$$V_3 = \frac{1}{2}(e_x^2 + e_y^2).$$

ومشتقتها:

$$\dot{V}_3 = -a e_x^2 + e_y^2(c - z) + c e_x e_y.$$

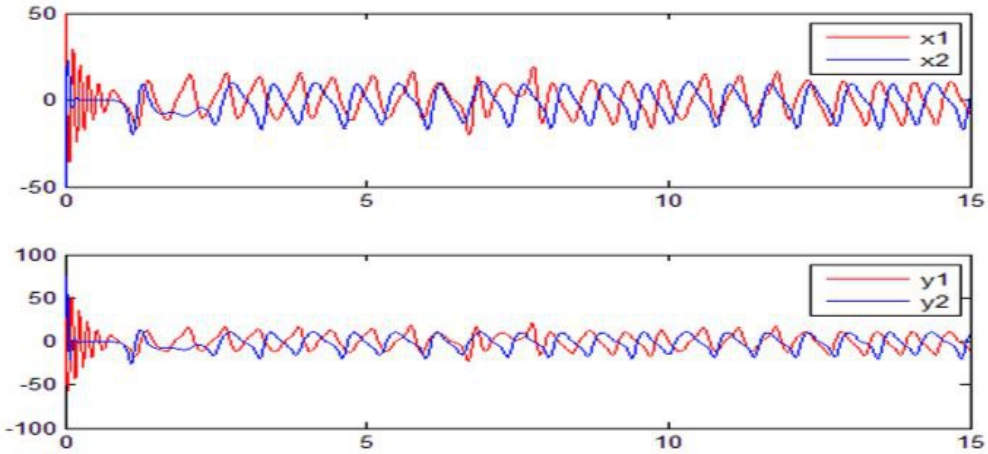
لكي يتزامن النظامان (4.7) و (4.8)، يكفي أن يكون:

$$\dot{V}_3 < 0.$$

محاكاة عددية: (نفس القيم السابقة)

من أجل القيم: $(a; b; c) = (35; 3; 28)$

والقيم الابتدائية: $(x_1; y_1; z_1) = (50, 35, 50)$; $(y_2; z_2) = (-50, 29)$



شكل 3.4: التزامن المطابق لنظام Chen عندما يكون z هو الإشارة المرسِلة.

خاتمة

تناولت هذه المذكرة العلاقة بين علم التشفير والأنظمة الفوضوية، من خلال أربعة فصول مترابطة. بدأنا بتقديم لمحة عامة عن علم التشفير وأنواعه، ثم انتقلنا لدراسة خصائص الأنظمة الديناميكية والفوضوية. بعد ذلك، تطرقنا إلى تزامن الأنظمة الفوضوية كخطوة أساسية نحو استخدامها في التشفير. وفي الأخير، قمنا بتطبيق عملي لمزامنة نظام Chen باستخدام طريقة Carroll و Pecora ، مما أبرز الإمكانيات التطبيقية لهذه المفاهيم. تُظهر هذه الدراسة أن الأنظمة الفوضوية تمثل أداة واعدة في تطوير تقنيات تشفير أكثر تعقيدًا وأمانًا. ختامًا، يمكن طرح السؤال التالي: **ما فائدة تزامن الأنظمة الفوضوية؟**

الجواب: هو أن هذا الظاهرة لها تطبيقات متعددة، خصوصًا في مجال **الاتصالات الرقمية**. مع التطور السريع للتقنيات الحديثة، وبروز مشاكل سرية التبادلات، يتبيّن أن **الخصائص الجوهرية للفوضى** — كالعشوائية والحساسية الشديدة للظروف الابتدائية — يمكن أن تُستخدم كوسيلة فعالة لتحسين أمن الاتصالات.

قائمة المراجع

[1] Afraimovich V.S., Verichev N.N., Rabinovich M.I., Stochastic synchronization of oscillation in dissipative systems, Radiophysics and Quantum Electronics, vol. 29, no. 9, pp. 747–751, 1986.

[2] Chen G., Dong X., From Chaos to Order Methodologies Perspectives and Applications, World Scientific, 1998.

[3] Fujisaka H., Yamada T., Stability theory of synchronized motion in coupled-oscillator systems, Progress of Theoretical Physics, vol. 69, no. 1, pp. 32–47, 1983.

[4] Gajić Z., Qureshi M.T.J., The Lyapunov Matrix Equation in System Stability and Control, Academic Press, 1995.

[5] Gasri A., Chaos et synchronisation généralisé dans les systèmes dynamiques, Doctorat en Mathématiques, Université Constantine 1, 2018.

[6] Kassem A., Protocoles gestion et transmission sécurisée par chaos des clés secrètes Applications aux standards TCP IP via DVB S UMTS EPS, École doctorale Sciences et Technologies, Liban, 2013.

[7] Kerckhoffs A., La cryptographie militaire, Journal des sciences militaires, 1883.

[8] Khalil H.K., Nonlinear Systems third edition, Prentice Hall, 2002.

[9] Menacer T., Synchronisation des systèmes dynamiques chaotiques à dérivées fractionnaires, Doctorat en Sciences Mathématiques, Université Constantine 1, 2014.

[10] Michel A.N., Hou L., Liu D., Stability of Dynamical Systems Continuous Discontinuous and Discrete Systems, Birkhäuser, 2008.

[11] Pecora L.M., Carroll T.L., Synchronizing nonautonomous chaotic circuits, IEEE Transactions on Circuits and Systems II Analog and Digital Signal Processing, vol. 40, no. 10, pp. 646–650, 1993.

[12] Slotine J.J.E., Li W., Applied Nonlinear Control, Prentice Hall, 1991.