Mise en place d'un cryptosystème d'EL Gamal sur les courbes elliptiques et étude comparative de sa sécurité

Liste des membres du groupe

— DENEUX Rafael
— COMMUNAL Hugo

Positionnements thématiques

— Mathématiques (Algèbre, Théorie des groupes, Coubres elliptiques)
— Informatique (informatique théorique, Python, C)

Mots-clés

— Simulation numérique
— cryptographie
— complexité algorithmique
— groupes cycliques
— logarithme discret
— courbes elliptiques

Bibliographie commentée

lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

forme de Weierstrass des courbes elliptiques

La forme de Weierstrass des courbes elliptiques s'écrit :

$$\frac{d^2x(t)}{dt^2} - \varepsilon\omega_0 \left(1 - x^2(t)\right) \frac{dx(t)}{dt} + \omega_0^2 x(t) = 0$$

avec :

— ε : paramètre de non-linéarité modulant l'intensité de l'amortissement négatif,

— ω_0 : pulsation propre du système.

Cette équation n'étant pas résolvable analytiquement du fait du coefficient non constant du terme d'ordre un, l'utilisation de simulations numériques est nécessaire afin d'obtenir des solutions approchées de $x(t)$.

L'existence des comportements limites de cet oscillateur peut être prouvée par le théorème de Poincaré–Bendixson, qui stipule que soit $x(t)$ converge vers une limite, soit son comportement asymptotique est une fonction périodique appelée *cycle limite*. Ce phénomène constitue un exemple typique d'oscillations auto-entretenues.

Approche numérique et expérimentale

Il est possible de mettre en œuvre des systèmes électriques utilisant des amplificateurs opérationnels, des condensateurs et des bobines, mais également de simuler ce comportement à l'aide d'outils numériques. Une résolution utilisant des langages de programmation tels que Python permet une approche simple et efficace du phénomène.

Les simulations permettent notamment d'obtenir des résultats concernant :

— les cycles limites,

— la durée du régime transitoire,

— la période des oscillations.

Une approche visuelle est également possible grâce aux diagrammes de phase représentant $\frac{dx}{dt}$ en fonction de x. Le caractère attractif du cycle limite permet de prédire certains comportements à partir des isoclines.

Oscillateur de Van der Pol forcé

Une seconde version de l'équation, dite *forcée*, s'écrit :

$$\frac{d^2x(t)}{dt^2} - \varepsilon\omega_0 \left(1 - x^2(t)\right) \frac{dx(t)}{dt} + \omega_0^2 x(t) = \omega_0^2 X \cos(\omega t)$$

Cette version conduit à des comportements chaotiques, sensibles aux conditions initiales et non prévisibles à long terme, étudiés dans le cadre de la théorie du chaos déterministe.

Problématique retenue

Comment les oscillateurs de Van der Pol permettent-ils d'illustrer l'existence et les caractéristiques de cycles limites dans des systèmes dynamiques non linéaires ?

Objectifs du TIPE

— Simulations numériques pour différentes valeurs de paramètres

— Mise en place d'un dispositif expérimental sous forme de circuit électrique

— Interprétation et exploitation des résultats expérimentaux

— Preuve de l'existence du cycle limite à l'aide du théorème de Poincaré–Bendixson

Références

Références

[1] Théorème de Poincaré–Bendixson — Wikipédia

[2] J. Gleick, *Chaos : Making a New Science*, Flammarion, 1988.

[3] B. Van der Pol, J. Van der Mark, *The Heartbeat considered as a Relaxation Oscillation*, Philosophical Magazine, 1928.

[4] F. C. Moon, *Chaotic Vibrations*, Wiley, 1992.