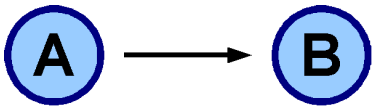
Forschungsmodul: Komplexe Systeme

Bericht zur Vorlesung vom 17. Januar 2008 von Jan-Philip Gehrcke

---

Chaossynchronisation

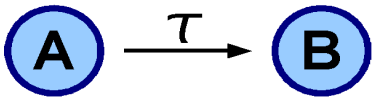


Gegeben seien zwei dynamische zeitabhängige Systeme a und b, die durch einen Kopplungsterm miteinander verknüpft sind. Sie bilden folgendes Gleichungssystem:

$$a_t = f(a_{t-1})$$
$$b_t = (1-\epsilon)\, f(b_{t-1}) + \epsilon\, f(a_{t-1})$$

Dabei ist $f(x)$ die logistische Abbildung $f(x) = rx(1-x)$ mit $r = 4$, also chaotischem Verhalten.

Eine offensichtliche Lösung des Gleichungssystems ist die synchrone Trajektorie $a_t = b_t$. Das bedeutet, dass die Systeme zu jeder Zeit im Gleichtakt sind. Die chaotischen Eigenschaften jedoch bleiben erhalten, sodass hier sogenannte Chaossynchronisation auftritt. Eine Stabilitätsbetrachtung der Lösung bei kleinen Abweichungen $b_t = a_t + d_t$ liefert, dass die Synchronisation der Systeme für $\epsilon > 1/2$ gewährleistet ist.

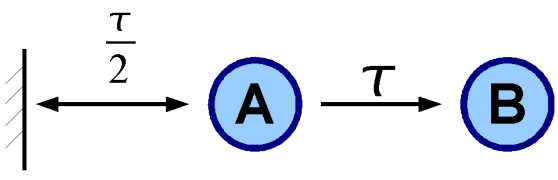


Möchte man das Phänomen der Chaossynchronisation für Verschlüsselungszwecke benutzen, so wird in der Realität zwischen zwei Systemen, die Informationen austauschen, eine Strecke liegen und somit eine Verzögerung existieren. Die Untersuchung des obigen Modells mit der Modifikation einer Verzögerungszeit τ zwischen den beiden Systemen ergibt, dass $b_t = a_{t-\tau+1}$ eine Lösung ist (bei gleicher Stabilitätsbedingung).

Die angesprochene Verzögerung (Delay) ergibt sich zum Beispiel bei der Chaossynchronisation zwischen Lasern, welche ein aktueller Ansatz bei der Suche nach der perfekt verschlüsselten Informationsübertragung ist. Die interne zeitliche Dynamik eines Lasers ist viel schneller als das Laserlicht auf einer denkbar sinnvollen Strecke, weshalb der Effekt des Delays ernstzunehmen ist.

Im Folgenden sollen idealisierte 1-Moden-Laser betrachtet werden. Die Dynamik des Lasers ist dann durch drei gewöhnliche Differentialgleichungen (für Amplitude, Phase und Population) beschreibbar. Nach einem Einschwingvorgang verbleibt ein solches Lasersystem bzw. die Strahlung in einem festen Zustand (konstante Frequenz). Führt man das ausgesendete Signal zurück auf den Laser, unterliegt die Intensität der Strahlung einer chaotischen Dynamik. Es entsteht Chaos durch verzögerte Rückkopplung.

Nun wird ein Lasersystem A betrachtet, welches auf sich selbst zurück- und an ein anderes Lasersystem B ankoppelt. Dabei sei die Verzögerungszeit $A \to A = A \to B = \tau$.



Für den Zustand der Systeme ergibt sich folgendes Gleichungssystem:

$$a_t = (1-\epsilon) f(a_{t-1}) + \epsilon f(a_{t-\tau})$$
$$b_t = (1-\epsilon) f(b_{t-1}) + \epsilon f(a_{t-\tau})$$

Trotz der zeitlichen Verzögerung bei der Informationsübertragung haben die Systeme hier wieder eine synchrone chaotische Trajektorie im Gleichtakt (Lösung $a_t = b_t$ mit Stabilitätsbedingung $\epsilon > 1/2$).

Nebenbemerkung: Nimmt man an, dass die Verzögerungszeit zwischen A und B kürzer ist als die Rückkopplungszeit bei A , eilt System B dem System A sogar voraus. Dies nennt man “anticipated chaos”.

Verschlüsselte Kommunikation

Für die Kryptographie bzw. verschlüsselte Kommunikation kann man die chaotische Intensität der Laserstrahlung ausnutzen und Information m mit geringer Amplitude aufmodulieren, ohne dass das Signal dadurch für einen externen Beobachter merklich anders (unchaotisch) aussieht. Koppelt man das Signal a von Laser A mit addierter Information m auf ihn zurück und an den Laser B , so ist $a_t = b_t$ wieder stabile Lösung des Gesamtsystems. Laser B bekommt also $a+m$ als Eingabe und strahlt selbst nur a ab. Die Differenz zwischen Ein- und Ausgang des Lasers B ist also genau m . Somit lässt sich die Information m fehlerfrei verschlüsselt übertragen.

Diese Form der Verschlüsselung (gerichtete Kopplung) ist jedoch nicht die Ideale. Unter Kenntnis der Laserparameter lässt sich die “Leitung abhören” und das Chaos herausfiltern und somit m bestimmen.

Prinzipiell ist man auf der Suche nach einem System, was unter die Kategorie der “public cryptography” fällt. Hierbei gibt es keine geheimen Parameter. Ein solches System ist von sich aus und auch bei allgemeiner Kenntnis über die

Funktionsweise ideal sicher. Seit Beginn der Erforschung der Quantenkryptographie ist erwiesen, dass ein solches System theoretisch möglich ist. Im Bezug auf Laserkryptotraphie ist bidirektionale Kopplung zwischen Lasern ein möglicher Weg zur “public cryptotraphy”.