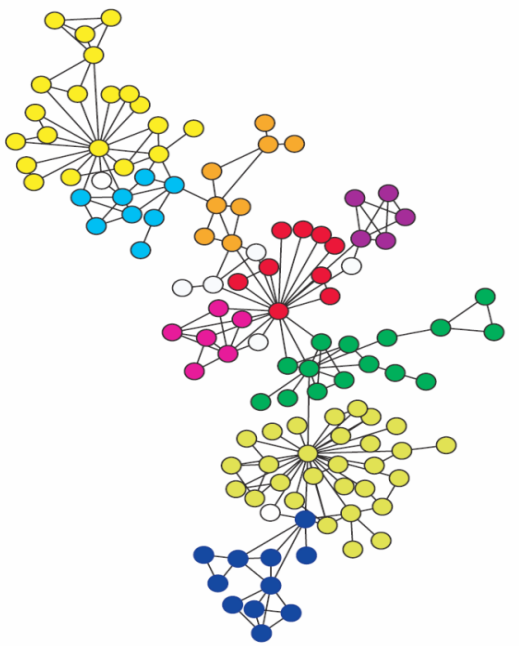
中国原子能科学研究院
China Institute of Atomic Energy
NSFC
60874087
10647001
70431002

探索基于束晕-混沌的网络保密通信



李永　刘强

复杂网络小组
中国原子能科学研究院，北京

Outline

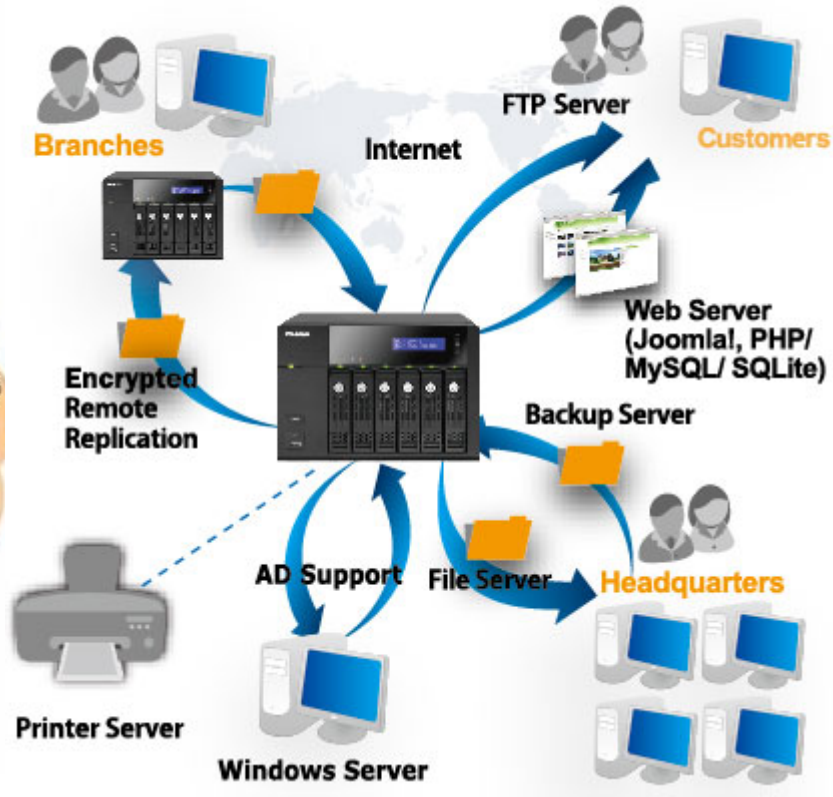
一. 引言

二.束晕-混沌保密通信电路设计原理

三.基于束晕-混沌的保密通信电路

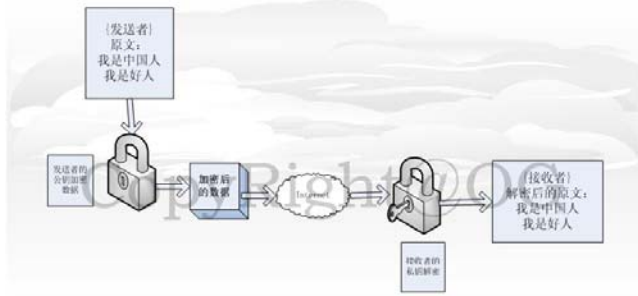
四. 小结

1. 引言



- 网络时代的数据传输频繁且传输数据量非常巨大，加密是保护信息安全的可行且有效的手段。

1. 引言



- 按照发展进程来看，密码包括古典密码、对称密钥密码和公开密钥密码等。目前在数据通信中使用最普遍的算法有DES 算法、RSA 算法等；
- 混沌通信具有许多优点：
  - 保密性强，因为具有宽带特性，特别是利用时空混沌增强抗破译、抗干扰(鲁棒性)能力；
  - 具有高容量的动态存储能力；
  - 具有低功率和低观察性；
  - 设备成本低等。
- 混沌保密通信已经成为保密通信的一个新的发展方向：
  - 基于混沌的非周期宽带连续频谱特性的扩谱通信；
  - 基于混沌复杂性的保密通信；
  - 基于混沌信号不相关的多用户通信。

2. 束晕-混沌保密通信电路设计原理

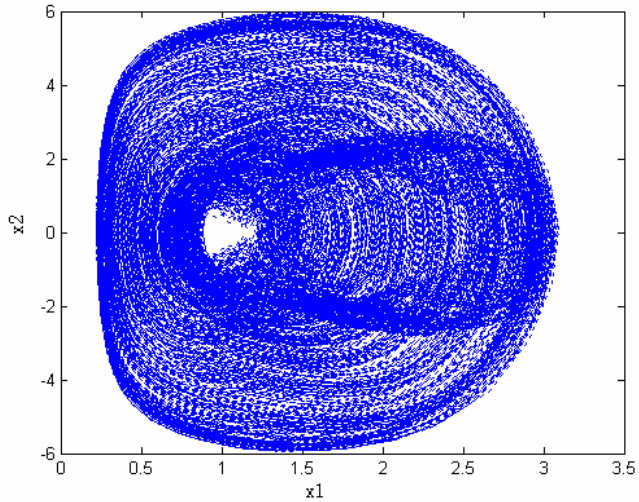
- 束晕-混沌离子束包络方程

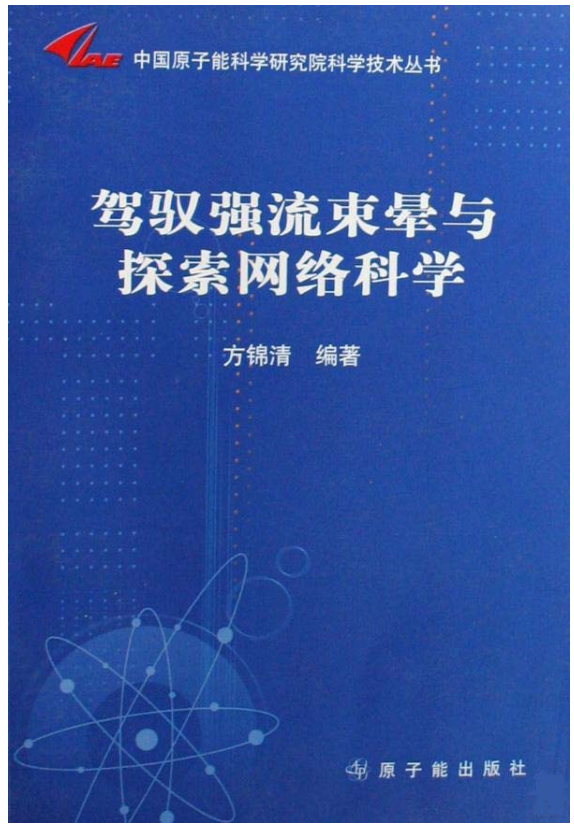
$$\frac{dx_1}{dt} = x_2$$

$$\frac{dx_2}{dt} = -(a + b\cos(x_3))^2 x_1 + \frac{K}{x_1} + \frac{1}{x_1^3},$$

$$\frac{dx_3}{dt} = \omega.$$

其中方程的参数分别取为：$a=1.65$, $b=1.25$, $w=2\pi$, $K=5$；当方程的初始条件$(x_1(0),x_2(0),x_3(0)) = (1.0, 0.5, 2\pi)$， 相空间（$x1,x2$）的相图处于混沌态如图所示。





2.1 驱动-响应同步

- 利用驱动-响应混沌同步方法将一个束晕-混沌振子作为驱动振子，另一个束晕-混沌振子作为响应振子，在x_2变量引入同步控制器G能够实现驱动振子和响应振子的完全同步，同步控制器G设计为：

$$G = g(x_2 - y_2)e^{q(x_2-y_2)^2}$$

- 其中g=0.02、q=10。
- 利用驱动-响应混沌同步方法，将驱动端的束晕-混沌信号作为加密信号，采用混沌掩盖的方式对原始信号进行加密得到密文信号，在响应端将加密信号与驱动端完全相同的解密信号进行解密，就可以恢复出明文信号，这样就为单向保密通信提供了理论基础。

2.2 小世界拓扑耦合同步

- 现实世界中的通信网络，例如互联网中计算机节点非常多，研究表明这些计算机节点所构成的复杂网络具有复杂网络的小世界特性，因此实现具有小世界拓扑的网络通信具有重要的实用价值和现实意义。
- 小世界网络中每个节点上引入束晕-混沌振子可得到具有小世界拓扑的束流传输网络，在束流传输网络中每个束晕混沌振子的x_2变量方程中引入耦合控制器，通过适当的耦合强度可实现束流传输网络的同步，引入耦合控制器后x_2变量方程如下式所示：

2.2 小世界拓扑耦合同步

$$\frac{dx_2}{dt} = -(a + b\cos(x_3))^2 x_1 + \frac{K}{x_1} + \frac{1}{x_1^3} + c\sum_{j=1}^{N} a_{i,j} H(x_j), \qquad i = 1, 2, \cdots, N$$

- 其中c为耦合强度；a_{ij}为具有小世界拓扑耦合网络的矩阵A（连接耦合变量）的矩阵元，这里仅考虑无向无权的网络，如果节点i和节点j之间有边相连接则$a_{ij}=a_{ji}=1$，否则$a_{ij}=a_{ji}=0 (i \neq j)$，耦合矩阵$A$是一个对称矩阵；

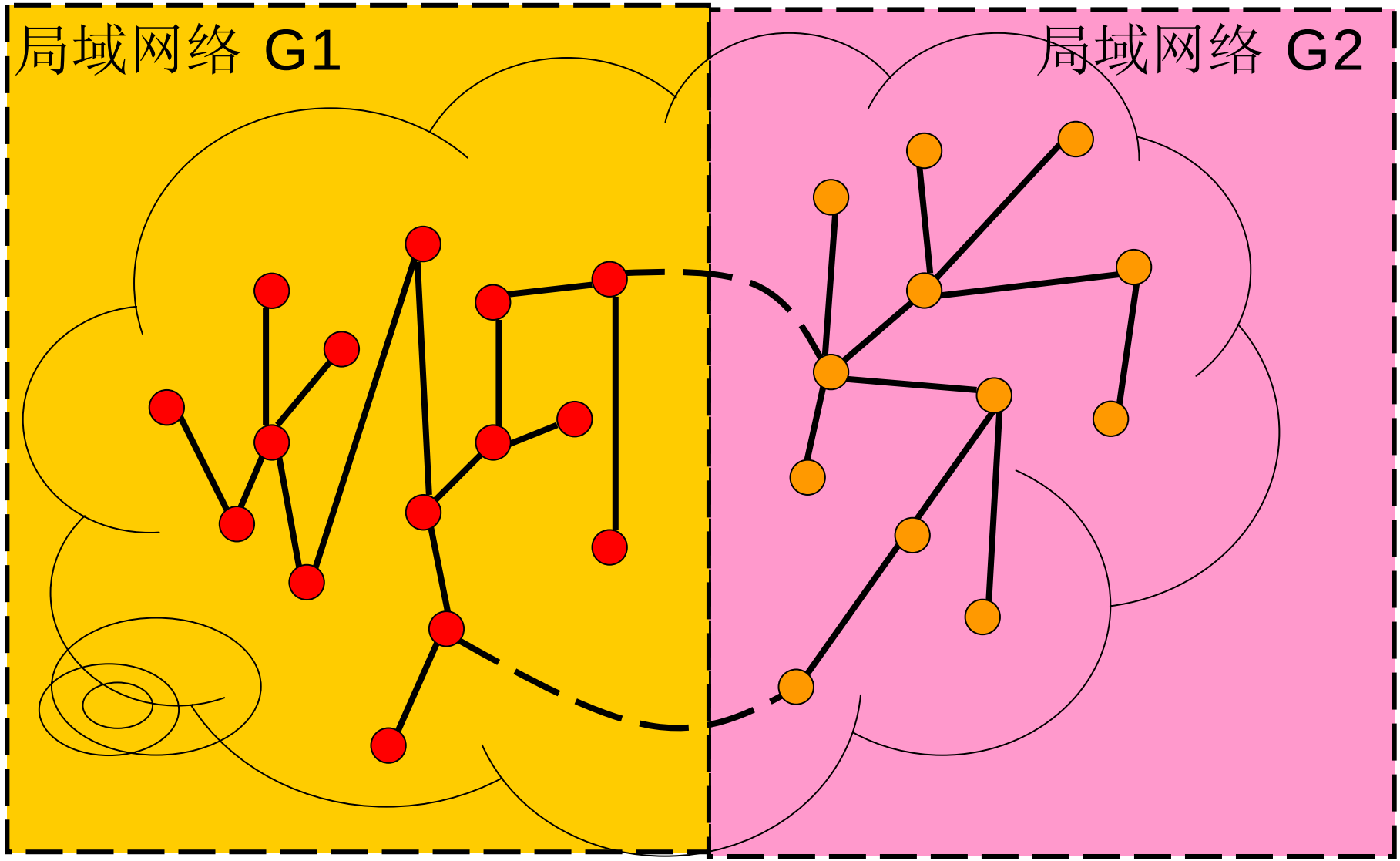
$$a_{ii} = -\sum_{\substack{j=1 \\ j\neq i}}^{N} a_{ij} = -\sum_{\substack{j=1 \\ j\neq i}}^{N} a_{ji} = -k_i, \quad i = 1, 2, \cdots\cdots N$$

- H是各个节点状态变量之间的内部耦合函数，也称为各个节点的输出函数。
- 当控制耦合强度取合适的值时可以很快将束晕振子控制到混沌态同步轨道，这样通过适当调整参数就可以达到对束流传输网络中所有束晕-混沌振子的同步控制目标。利用具有小世界拓扑的束流传输网络同步控制的方法，在通信网络中就能够实现对多个节点之间的保密通信。

2.3 多局域小世界拓扑耦合同步

- 现实社会中的许多复杂网络通常由多个“社区”、“群落”或“模块”等构成，根据不同特性、目标，一个复杂网络可以划分为多个局域网络。
- 例如互联网就是一个由很多不同层次的、地域的局域网络组成的具有小世界拓扑的多局域网络。
- 实现多局域网络之间的束流传输网络的同步控制，对于在多个通信网络之间进行保密通信更有实际意义。

2.3 多局域小世界拓扑耦合同步



2.3 多局域小世界拓扑耦合同步

- 分别在局域世界G1和G2中分别加入耦合控制，x_2变量方程如式所示。

$$\dot{x}_i = f(x_i) + c\sum_{j=1}^{N_1} a_{i,j} h(x_j) \qquad i = 1, \cdots, N_1$$

$$\dot{x}_k = f(x_k) + c\sum_{j=N_1+1}^{N} a_{k,j} h(x_j) \qquad k = N_1 + 1, \cdots, N$$

- 我们的研究表明：当耦合强度c取合适值时，能够同时实现局域世界G1和G2中的束晕-混沌振子的同步。
- 多局域小世界拓扑耦合同步方法可为两个相对独立、但又有部分联系的通信网络之间进行保密通信提供了设计方案。

3. 基于束晕-混沌的保密通信电路

- 采用matlab的simulink工具箱作为电路仿真软件，分别设计基于上述设计方案的实际通信电路。

3.1 单个束晕-混沌振子电路

- 利用束晕-混沌振子方程组，其中常数a=1.65、b=1.25、ω=2π、K=5时出现束晕混沌态。

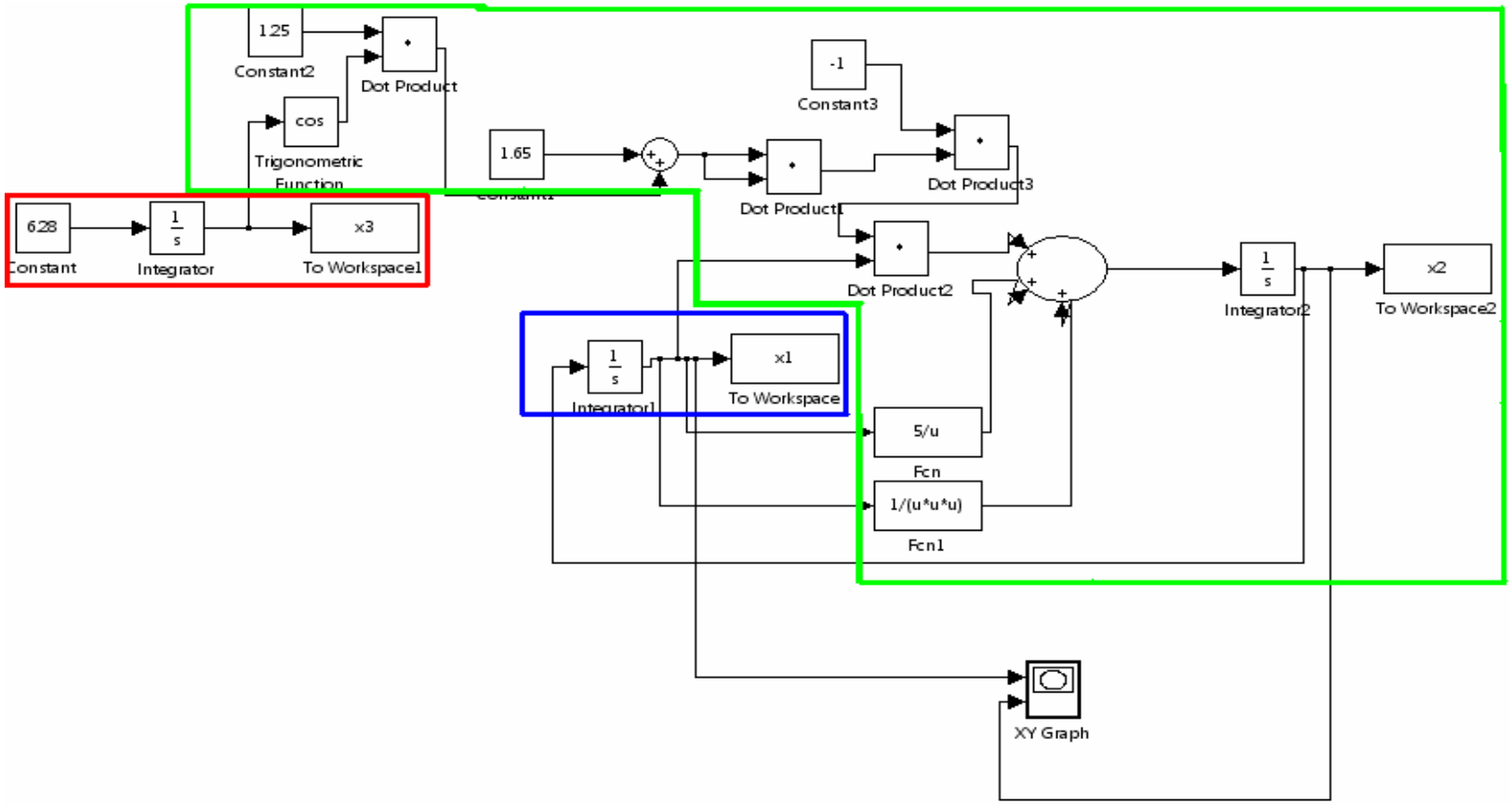
$$\frac{dx_1}{dt} = x_2$$

$$\frac{dx_2}{dt} = -(a + b\cos(x_3))^2 x_1 + \frac{K}{x_1} + \frac{1}{x_1^3},$$

$$\frac{dx_3}{dt} = \omega.$$

- 束晕-混沌振子方程组中加、乘、除、乘方、余弦、积分等计算，simulink 都有相应数学运算模块都已封装打包，搭建电路时只需按照方程组中的运算插入即可。

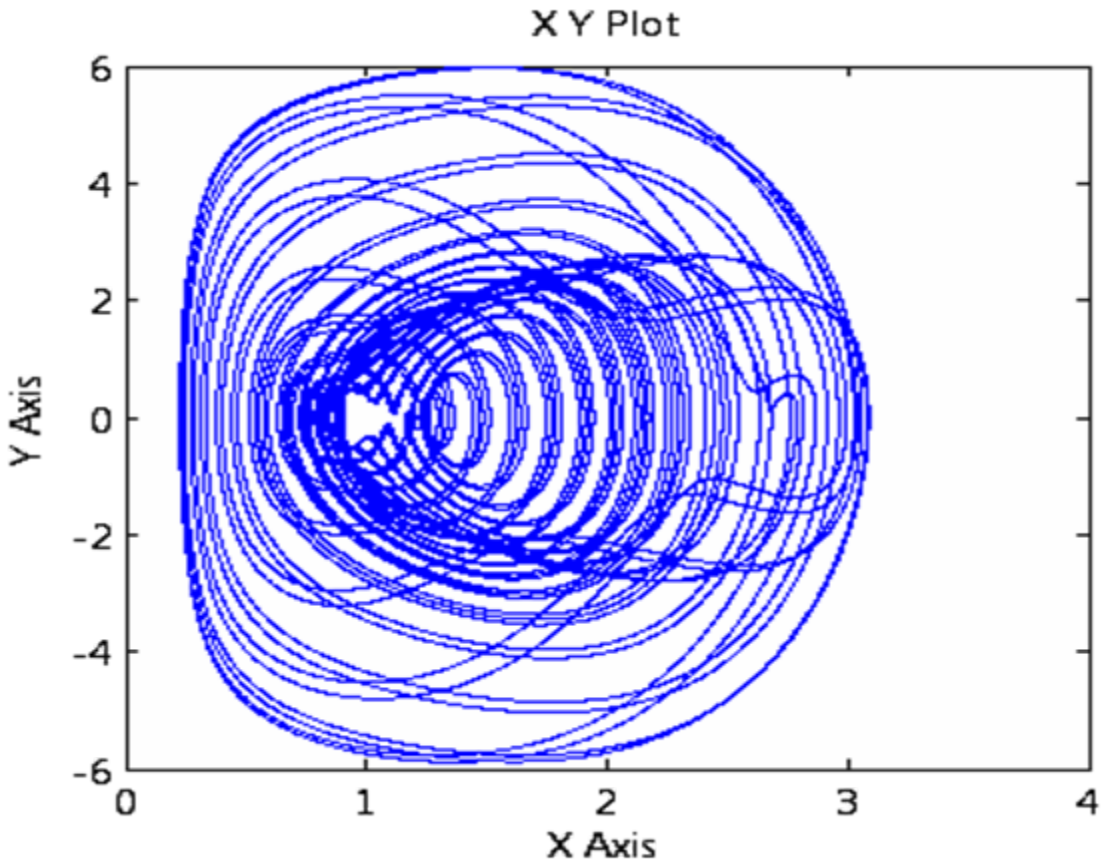
单个束晕-混沌振子电路图



- 图中蓝色线框内为束晕-混沌方程组中第一个变量x1的仿真电路；绿色线框内为x2的仿真电路；红色线内为x3的仿真电路。

单个束晕混沌振子x_1-x_2相图

- 将x_1、x_2作为信号源利用simulink中的画图模块（XY Graph）即可得到如图所示单个束晕混沌振子x_1-x_2相图。

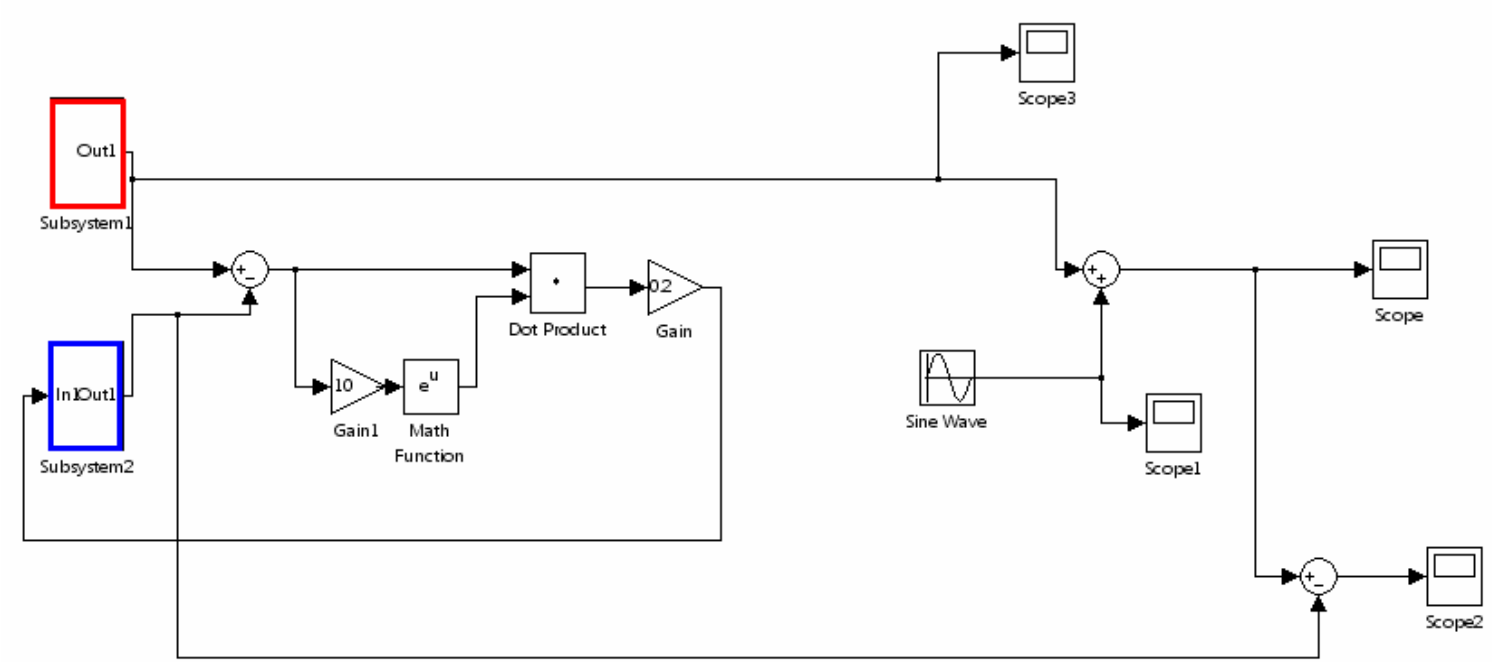


3.2 驱动-响应同步保密通信电路

- 当图中线路加入多个束晕-混沌振子时，可以想象电路会变得十分复杂，而且不易分辨清各个模块和线路之间的连接关系，因此我们将单个束晕-混沌振子电路中的各个模块归入到一个子系统（subsystem）中。
- Simulink中子系统的建立还能够在子系统加入Inport模块表示从子系统外部到内部的输入，加入Outport模块表示从子系统内部到外部的输出，这就为我们构建由多个束晕-混沌振子的电路提供了方便。

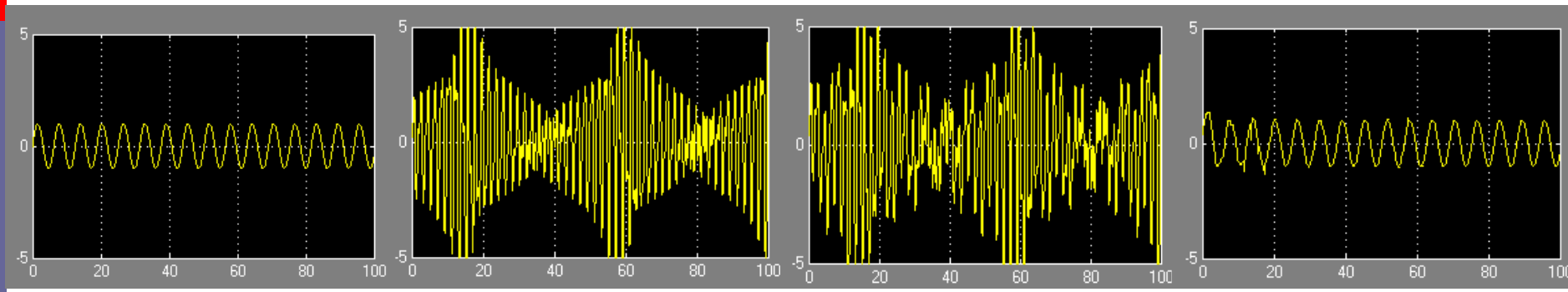
驱动-响应同步保密通信电路图

- 图中subsystem1模块（红色框）和subsystem2（蓝色框）模块分别为两个子系统即两个初值不同的束晕-混沌振子电路。
- 子系统1（subsystem1）有一个输出端作为驱动-响应同步电路的驱动端，子系统2（subsystem2）有一个输入端和一个输出端作为驱动-响应同步电路的响应端。驱动响应控制其方程G如式2所示。



对正弦信号进行加、解密过程

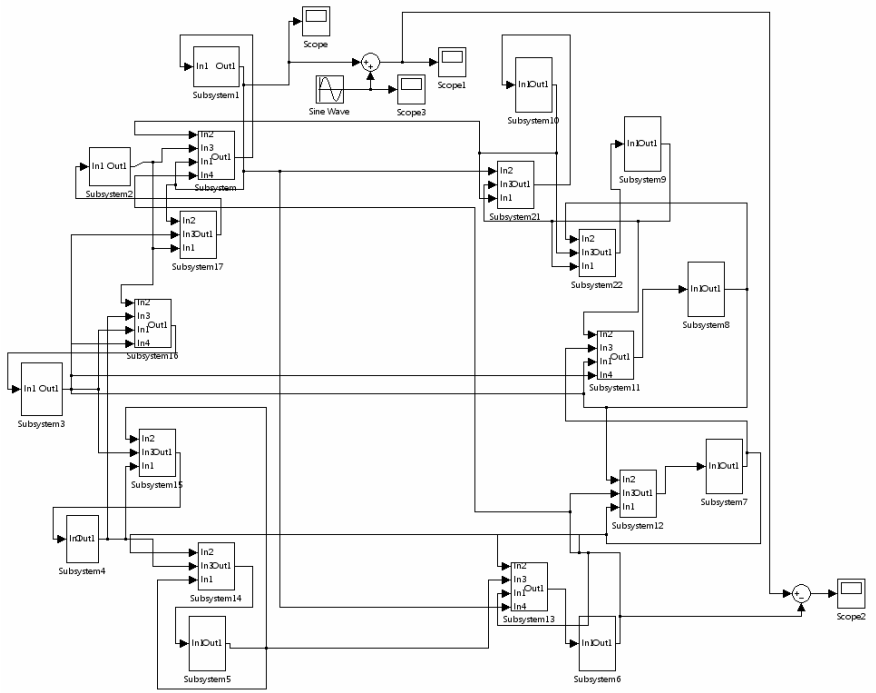
- 利用驱动-响应混沌同步信号对正弦信号进行加、解密过程
- 利用正弦信号作为原始信号，在利用驱动-响应电路的驱动端作为混沌信号对正弦信号相叠加进行加密，得到经过加密后的传输信号。利用驱动-响应电路的响应端的混沌同步信号作为解密信号对加密信号进行解密即可得到原始信号（正弦信号），分别将这四类信号分别连接到示波器模块进行显示。



(a)正弦信号　(b)混沌信号　(c)加密信号　(d)解密信号

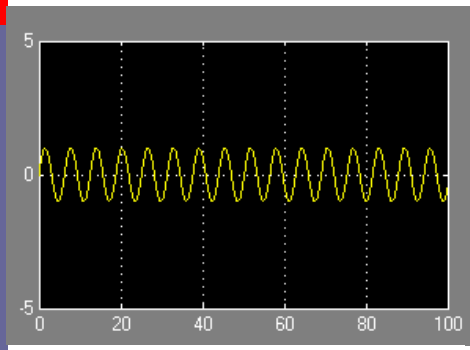
3.3 小世界拓扑耦合同步保密电路图

- 利用小世界同步控制的方法，通过全局耦合实现了小世界拓扑网络中每个束晕混沌振子的同步。
- 如果将同步信号作为加密信号对原始信号进行加密，那么可以在网络当中的任意两个节点之间都进行保密通信。
- 图为小世界拓扑混沌耦合通信电路图，我们在电路中加入了20个子系统即20个束晕-混沌振子，各个振子之间通过电路连接构成小世界耦合同步网络，可得到规模为20的小世界拓扑耦合同步保密通信电路。其中耦合强度c=2。

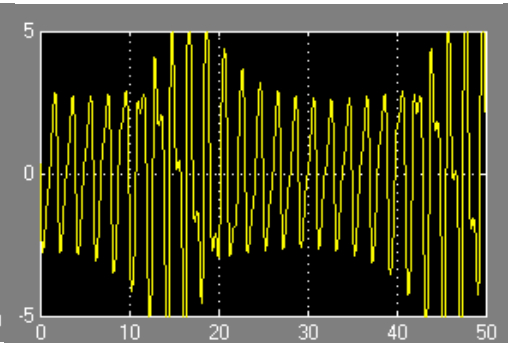


对正弦信号进行加、解密过程

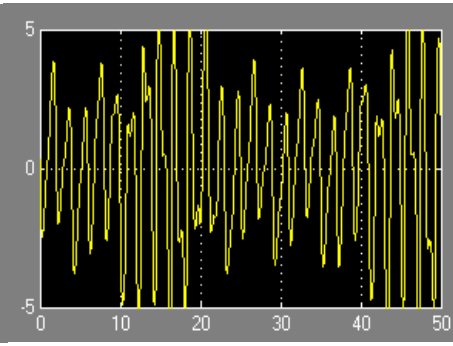
- 利用小世界耦合混沌同步信号对正弦信号进行加、解密过程：
- 利用正弦信号作为原始信号，利用小世界耦合混沌同步信号作为加密信号对正弦信号进行加密，得到经过加密后的传输信号。并且利用混沌同步信号作为解密信号对加密信号进行解密即可得到原始信号（正弦信号），分别将这四类信号分别连接到示波器模块进行显示，结果如图。



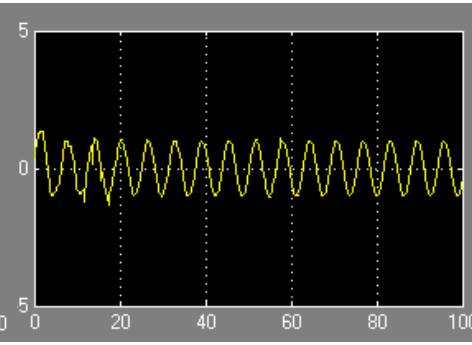
(a)正弦信号



(b)混沌信号



(c)加密信号

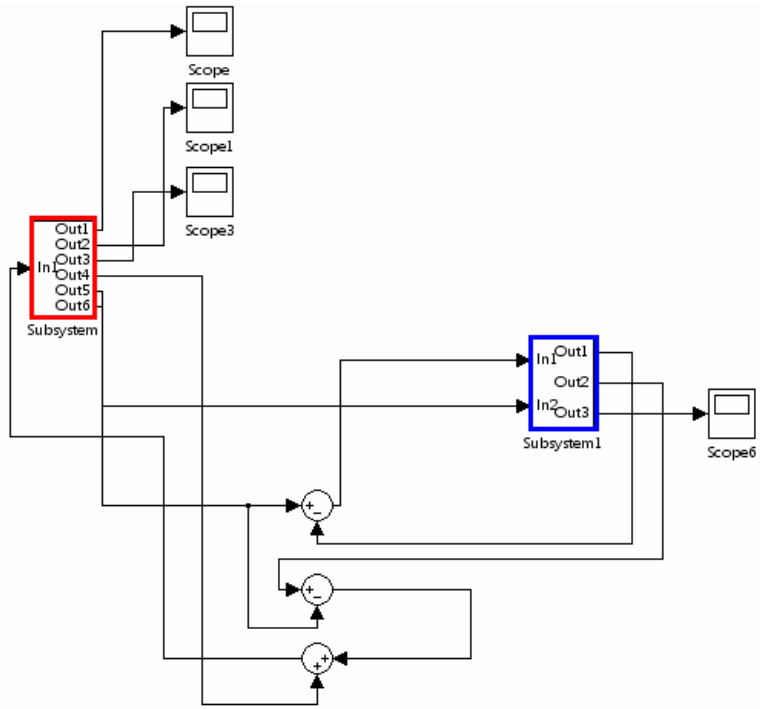


(d)解密信号

3.4 多局域小世界拓扑耦合同步保密通信电路

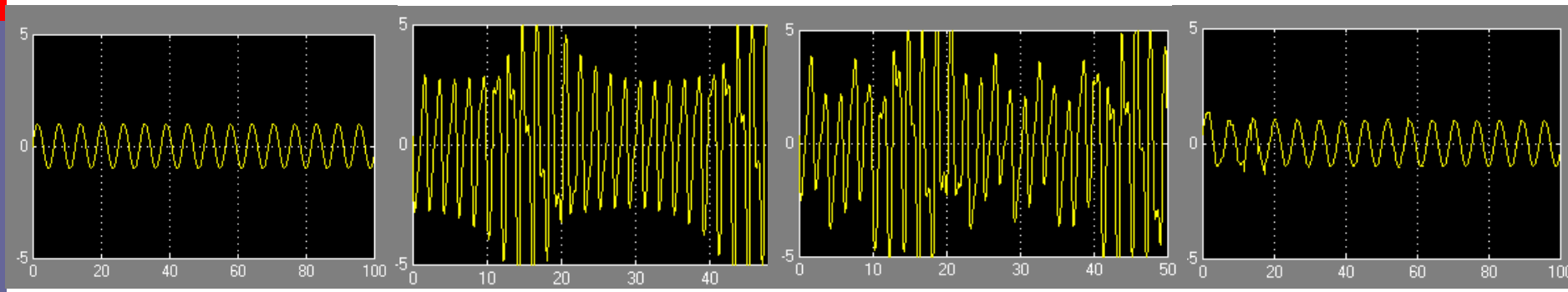
- 将小世界耦合同步保密通信电路组合成一个子系统，在电路中加入两个或多个这样的子系统，并在它们之间连接上少量的电路，即可以模拟多局域小世界网络的耦合电路图。

- 右图为我们所构建的多局域小世界拓扑耦合电路，图中红色部分为子系统1（局域世界1），蓝色部分为子系统2（局域世界2）。
- 局域世界1和局域世界2分别为两个独立的小世界耦合同步电路，规模均为20。
- 局域世界1和局域世界2之间有三条边相连，这样就构成了多局域小世界耦合电路。这样利用多局域小世界拓扑耦合控制就能够实现对电路中每个束晕混沌振子的同步控制得到同步信号。



对正弦信号进行加、解密过程

- 利用多局域小世界拓扑耦合同步信号对正弦信号进行加、解密过程：
- 以正弦信号作为原始信号，利用多局域小世界拓扑耦合同步信号作为加密信号对正弦信号进行加密，得到经过加密后的传输信号。并且利用混沌同步信号作为解密信号对加密信号进行解密即可得到原始正弦信号，分别将这四类信号分别连接到示波器模块进行显示，结果如图。

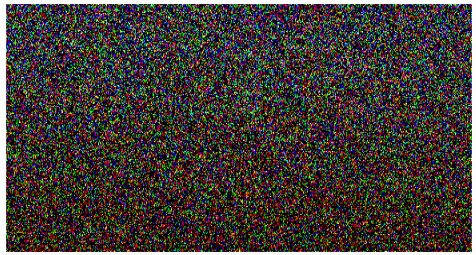


(a)正弦信号　(b)混沌信号　(c)加密信号　(d)解密信号

对图像文件的加密

- 多局域小世界拓扑耦合同步信号作为加密信号时对图像文件的加密。
- 图像文件经过混沌加密信号的加密之后与原始图像完全没有相似性。

(a)原始图像



（b）加密图像

（c）解密图像

小结

- 提出和设计了基于束晕-混沌同步的网络保密通信系统，设计了单个束晕振子的电路图，分别设计了三种通信方案：驱动-响应同步保密通信电路、小世界拓扑耦合同步保密通信电路以及多局域的小世界拓扑耦合同步保密通信电路。
- 电路仿真采用matlab中的simulink工具箱，通过模拟实验证明，这三种保密通信电路可以很好地实现了对于信号的加、解密，以及加密数据的传输。

中國原子能科學研究院
China Institute of Atomic Energy

NSFC

60874087
10647001
70431002

Thank you!