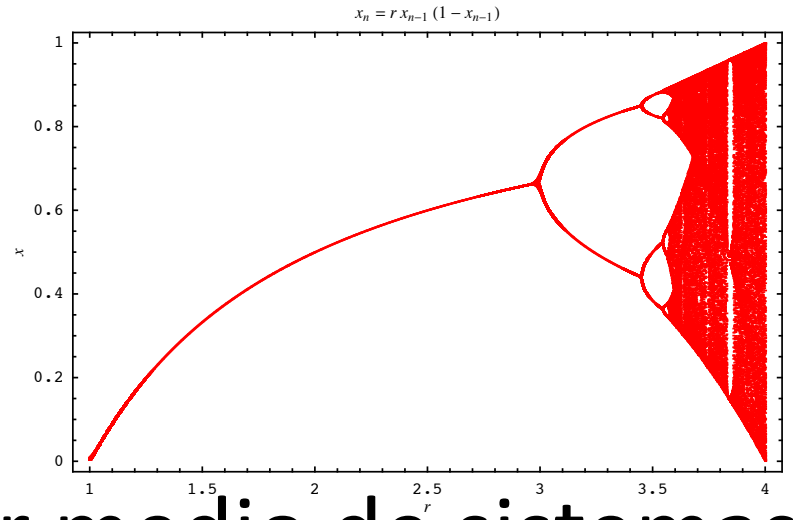


El cifrado por medio de sistemas complejos en estados no lineales

---

Hugo Solís

Motivación

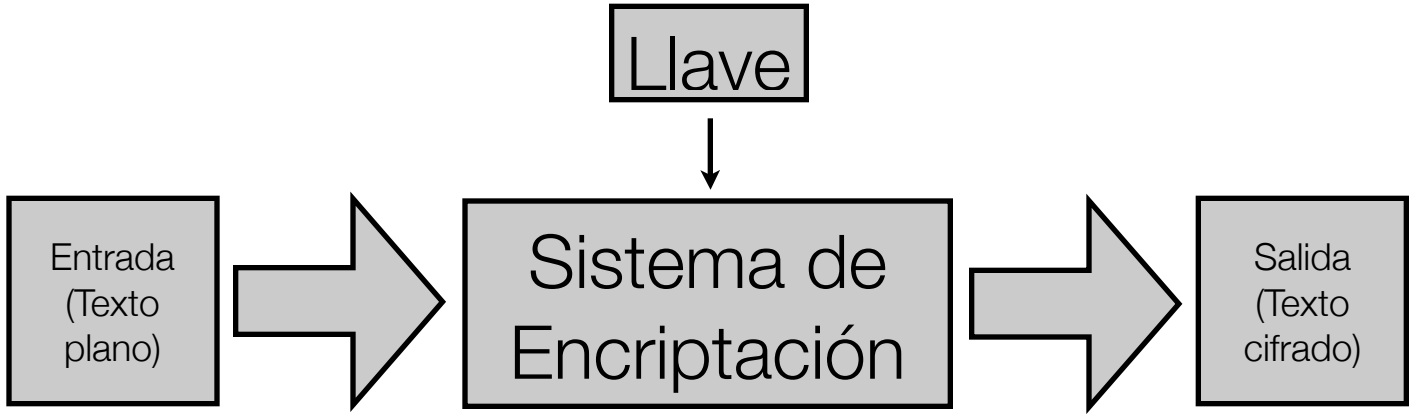
- RSA, Aggarwal & Maurer en 2009 prueban que romperlo en general es lo mismo que factorizar. (768 bits)

- Peter Shor en 1994 encuentra un algoritmo cuántico que permite factorizar en tiempos polinomiales números primos.

- Mayo 2013 Thermally assisted quantum annealing of a 16-qubit problem Nature Communications 4, 1903–1909

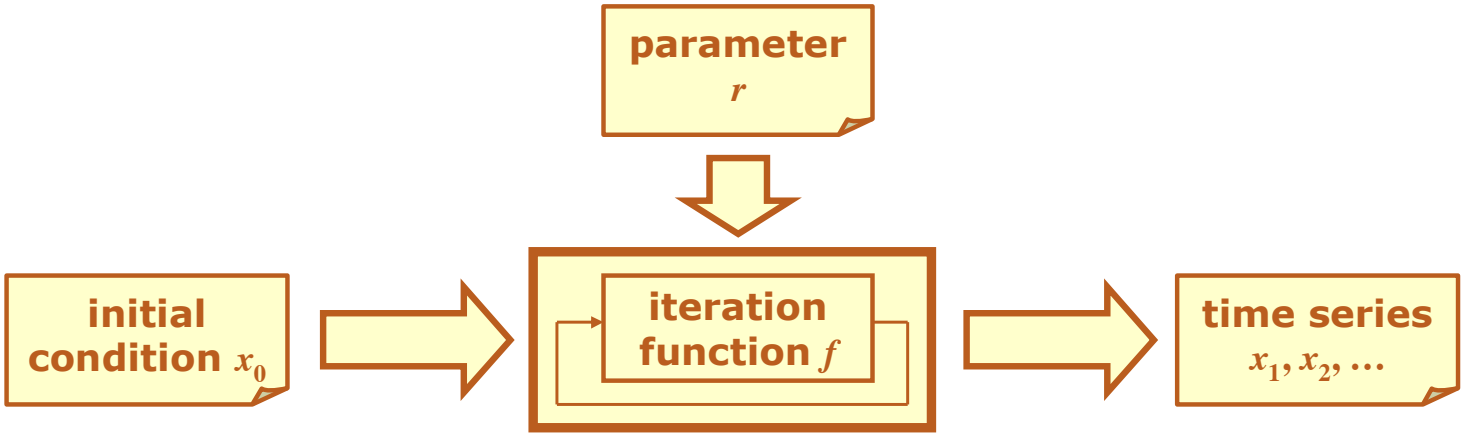
- Junio 2013 Experimental Quantum Computing to Solve Systems of Linear Equations. Phys. Rev. Lett. 110, 230501 (2013)

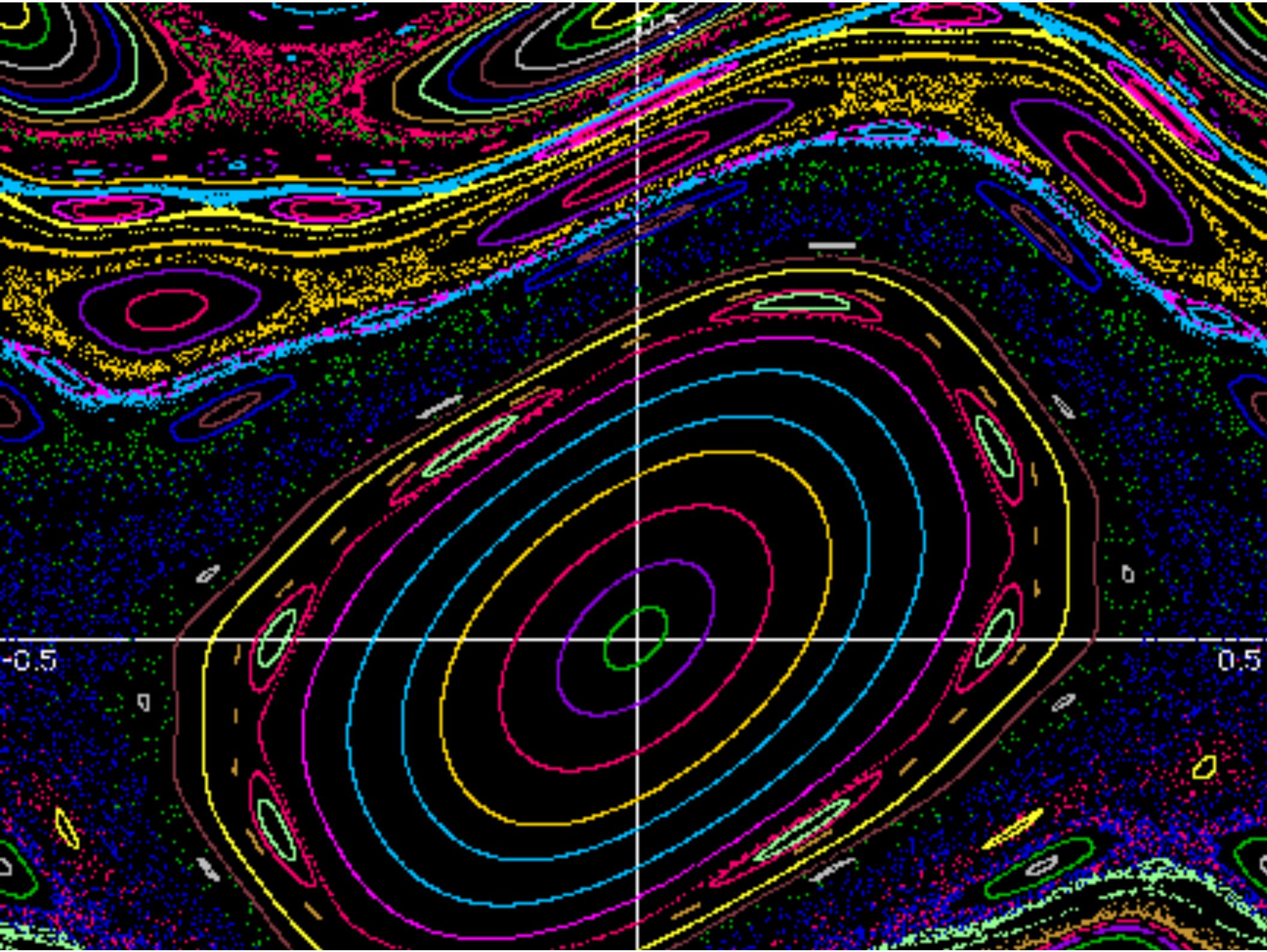
Cifrado


Llave
Entrada (Texto plano)
Sistema de Encriptación
Salida (Texto cifrado)

Encriptación Caótica

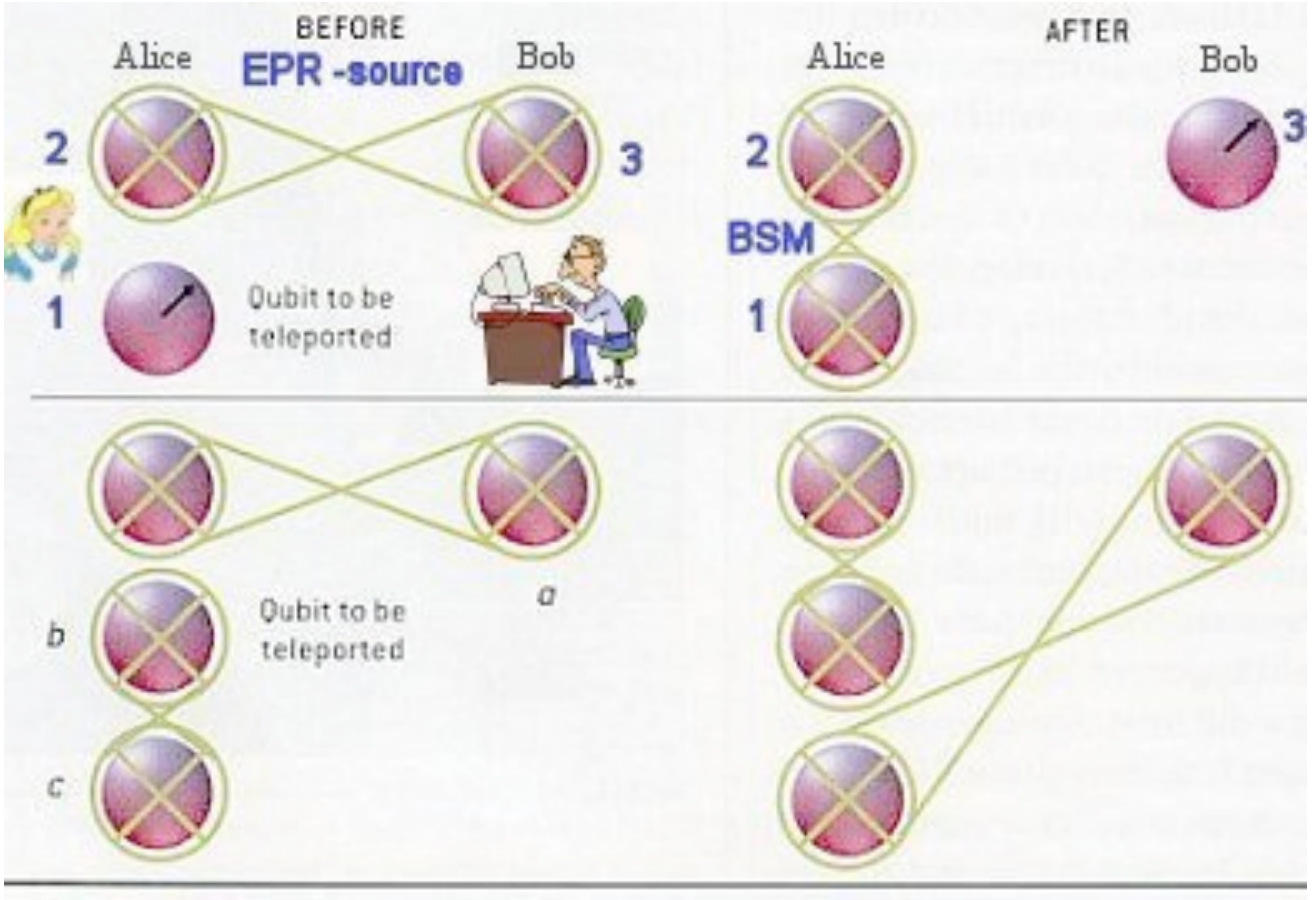
- Caos Determinista



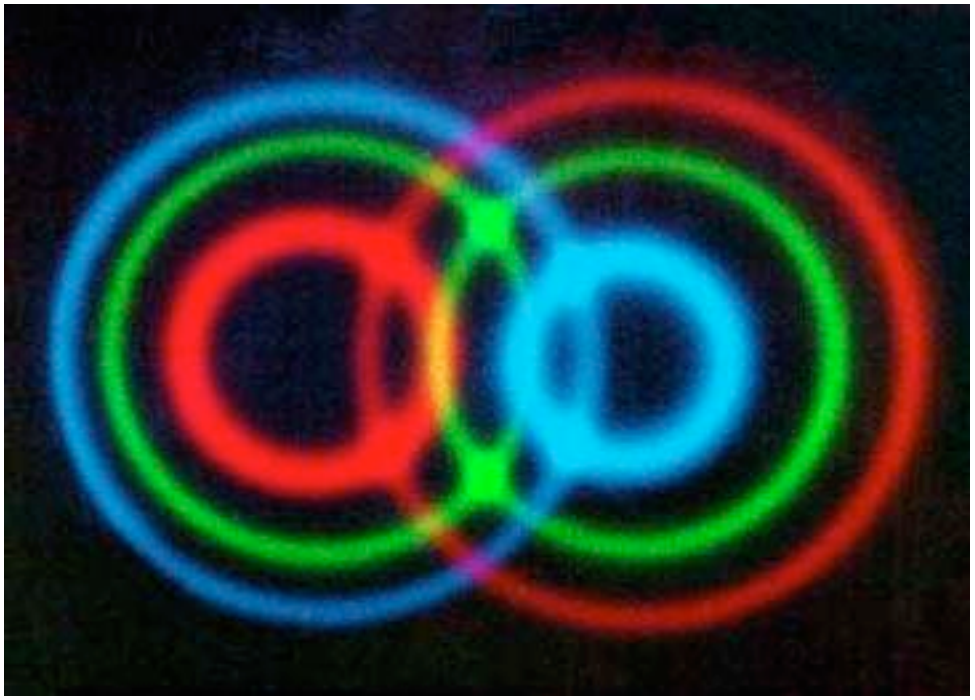

-0.5
0.5

Caso Cuántico

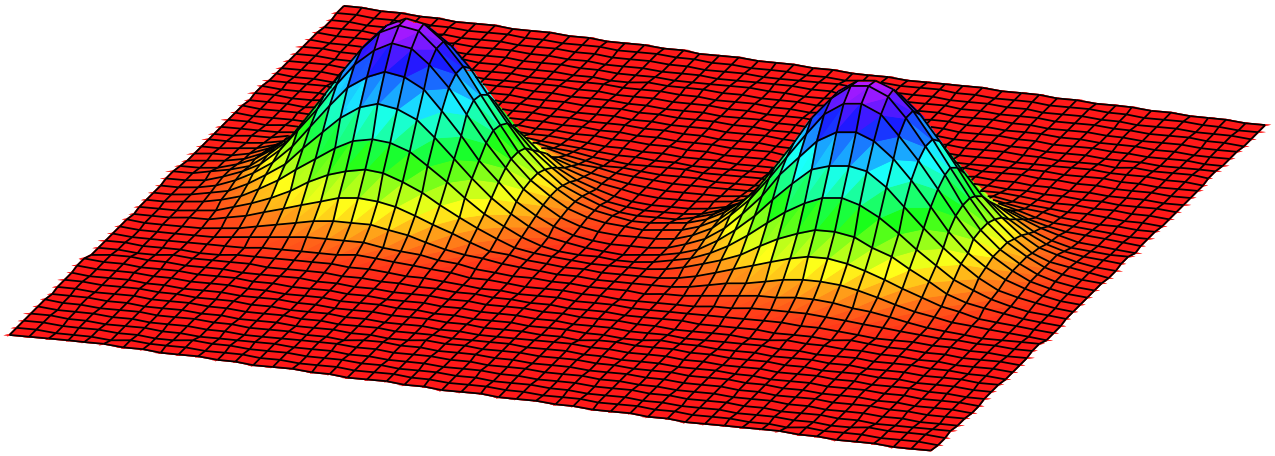
Cifrado hecho en un computador cuántico



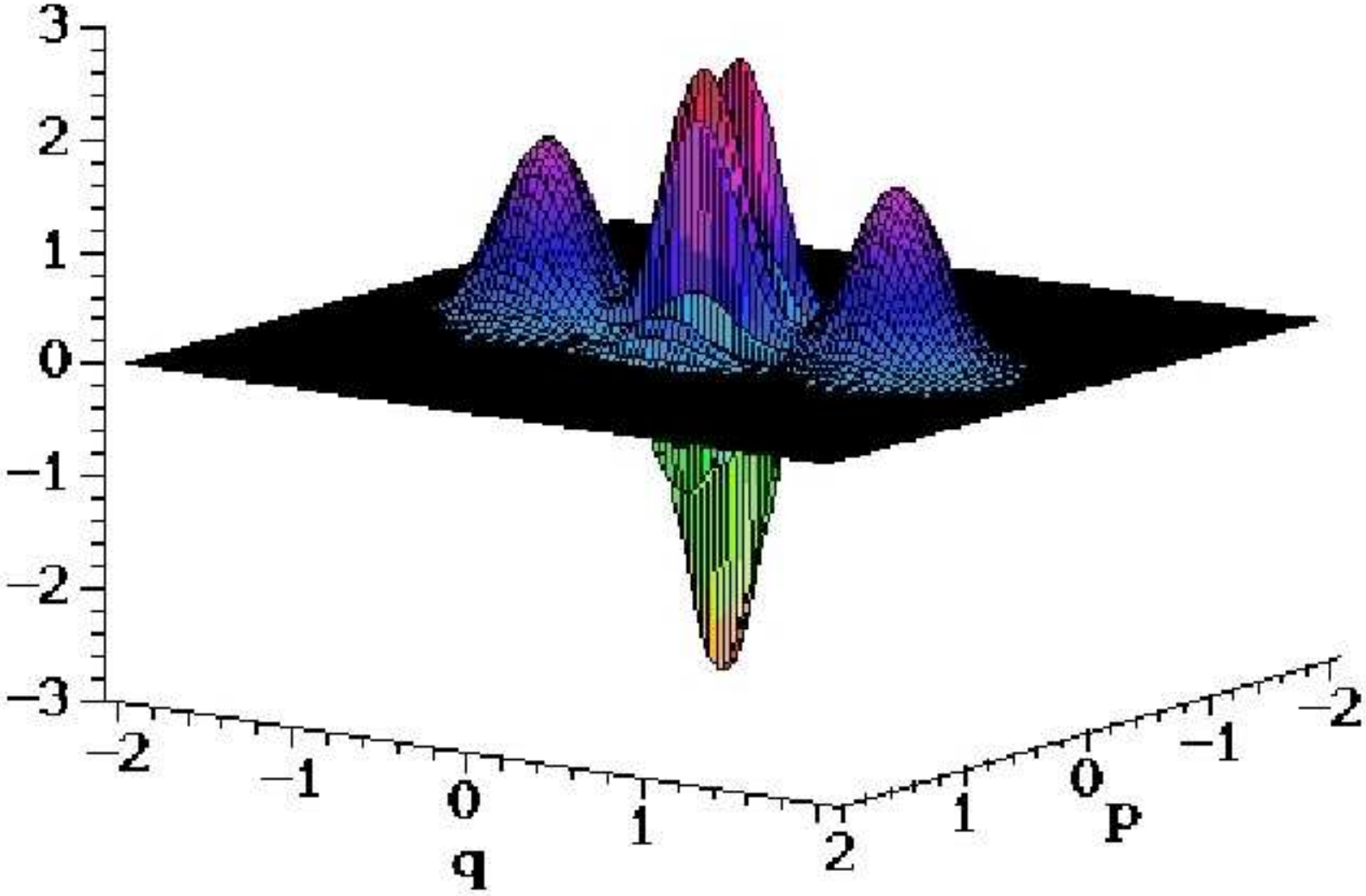
Enredo (Entanglement)



- No se entiende porque ocurre el enredo y varios opinan que pueda dar en sistemas clásicos.



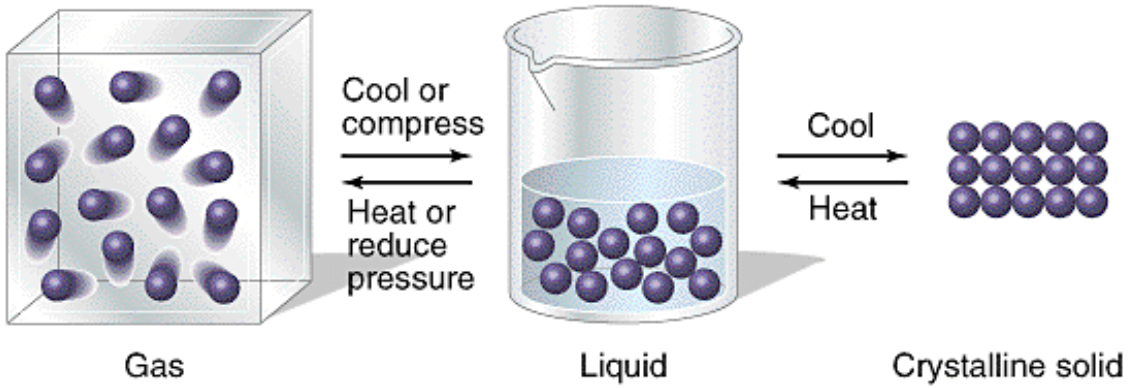
El gato



Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of modern physics*, *74*(1), 145-195.

Propuesta

- $$\frac{\partial C}{\partial t} = \frac{\partial}{\partial x}\left(C^3 \frac{\partial C}{\partial x}\right).$$



$$C(x,t) = \begin{cases} \dfrac{\left(A - \dfrac{3}{10}\dfrac{x^2}{t^{2/5}}\right)^{1/3}}{t^{1/5}}, & |x| \le t^{1/5}\sqrt{\dfrac{10}{3}A}, \\ 0, & |x| > t^{1/5}\sqrt{\dfrac{10}{3}A}. \end{cases}$$

ELSEVIER

Theoretical Computer Science 265 (2001) 79–108

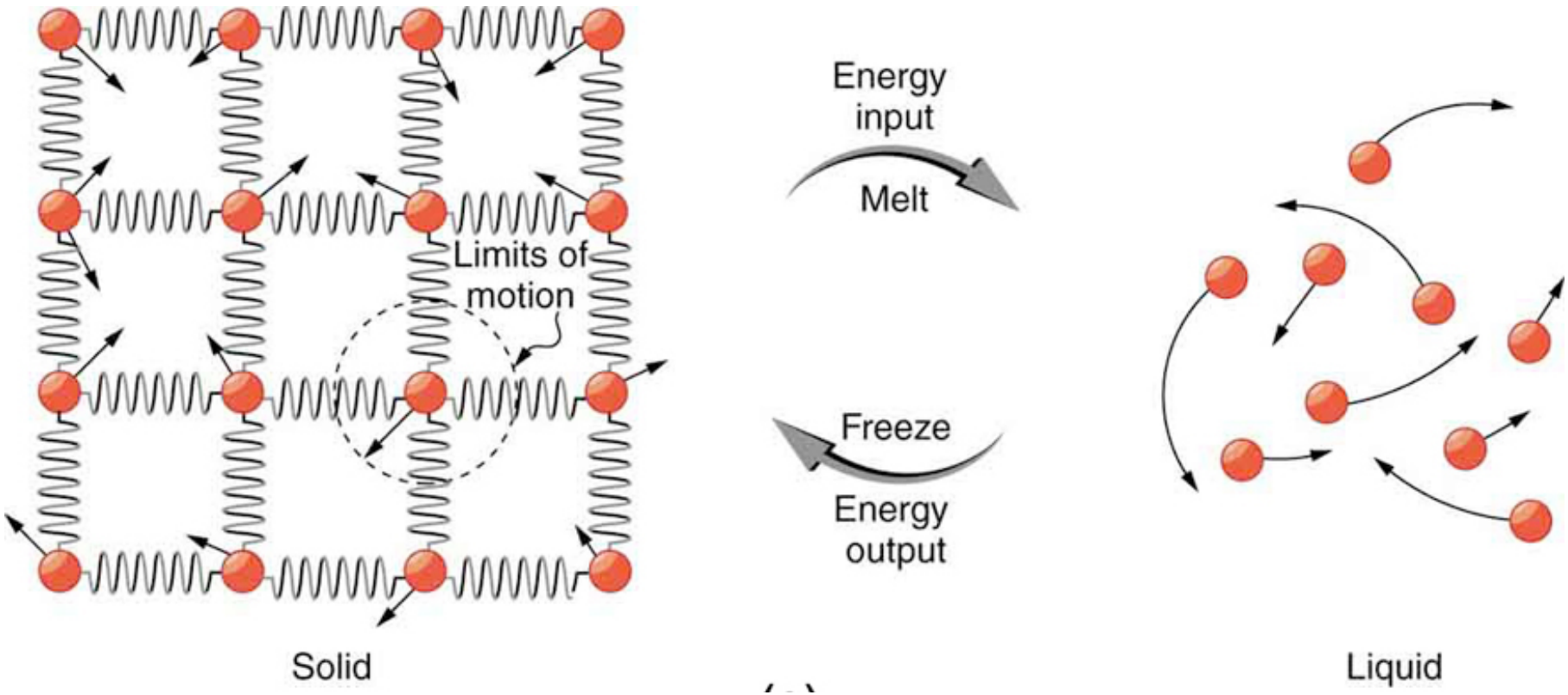
Theoretical Computer Science

www.elsevier.com/locate/tcs

A physicist's approach to number partitioning

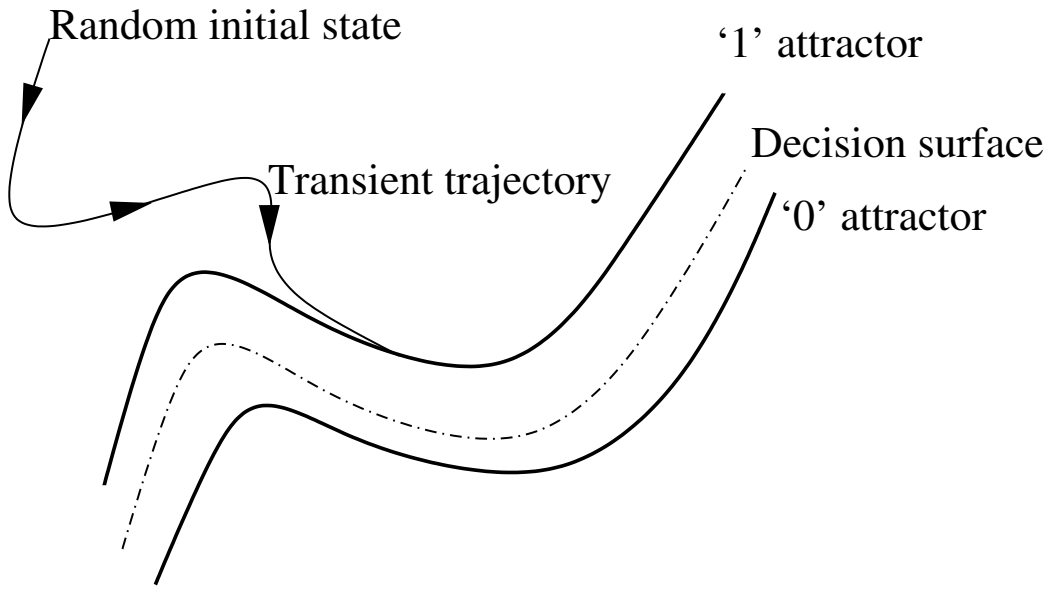
Stephan Mertens *

Institut für Theoretische Physik, Otto-von-Guericke-Universität, 39106 Magdeburg, Germany



El trabajo

- Existe un sistema clásico que presente un fenómeno similar al del enredo cuántico que sea útil para hacer cifrados resistentes al ataque cuántico.

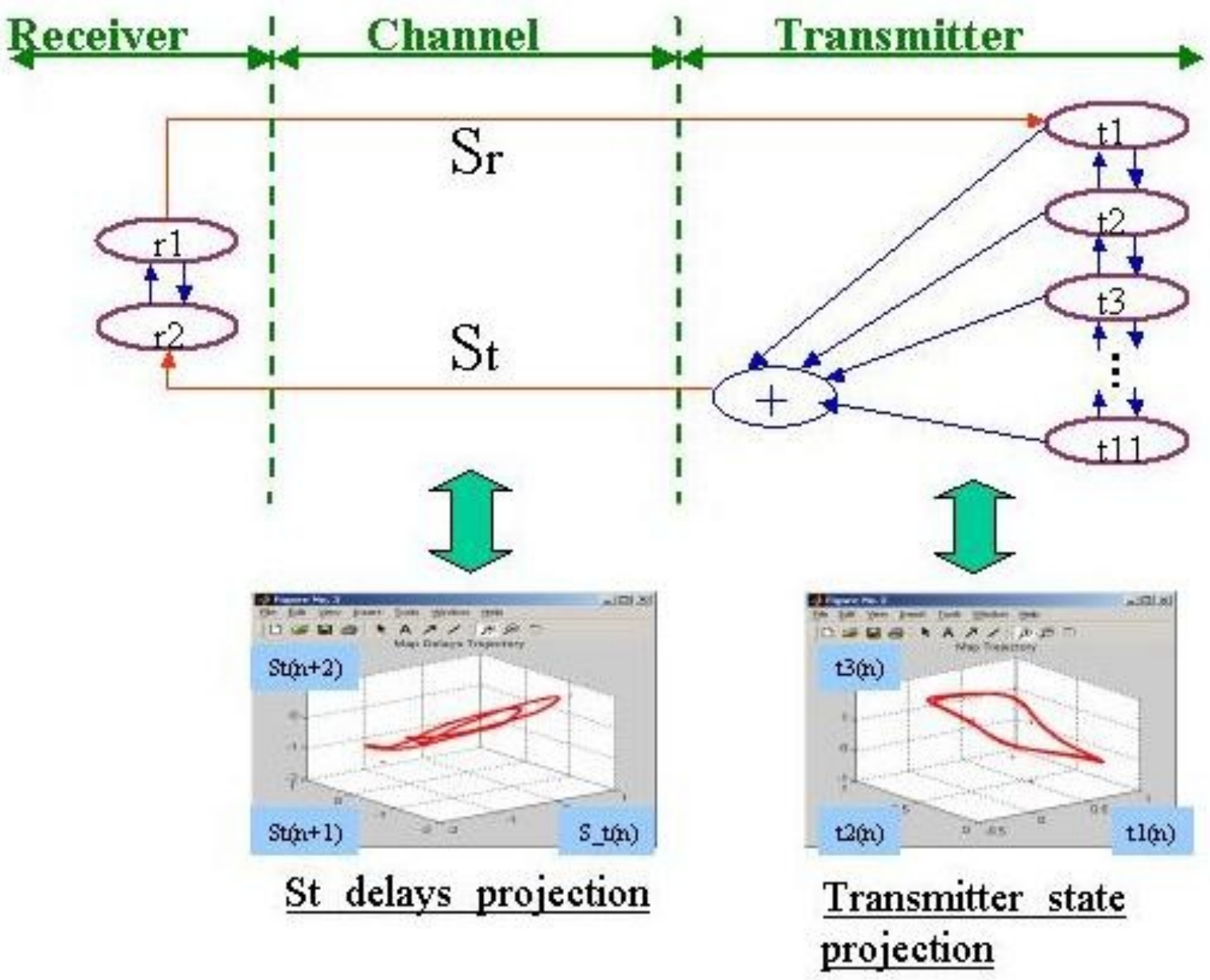


VOLUME 90, NUMBER 4 PHYSICAL REVIEW LETTERS week ending 31 JANUARY 2003

Using Distributed Nonlinear Dynamics for Public Key Encryption

Roy Tenny,[1,2] Lev S. Tsimring,[1] Larry Larson,[2] and Henry D. I. Abarbanel[1,3]
[1]*Institute for Nonlinear Science, University of California, San Diego, La Jolla, California 92093-0402*
[2]*Department of Electrical and Computer Engineering, University of California, San Diego, La Jolla, California 92093-0354*
[3]*Department of Physics and Marine Physical Laboratory (Scripps Institution of Oceanography), University of California, San Diego, La Jolla, California 92093-0402*
(Received 15 May 2002; published 28 January 2003)

$$\mathbf{t}(n+1) = \mathbf{F}_T(\mathbf{t}(n), s_r(n), m(n)),$$
$$\mathbf{r}(n+1) = \mathbf{F}_R(\mathbf{r}(n), s_t(n)),$$


Receiver
Channel
Transmitter
Sr
St
r1
r2
t1
t2
t3
t11
+
St(n+2)
St(n+1)
S_t(n)
t3(n)
t2(n)
t1(n)
St delays projection
Transmitter state projection