On the skew tent map as base of a new image chaos-based encryption scheme

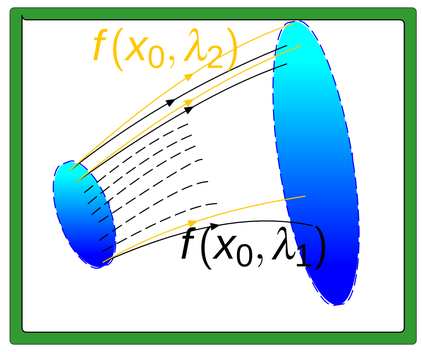
David Arroyo[1], Rhouma Rhouma[2], Gonzalo Alvarez[1], Veronica Fernandez[1] and Safya Belghith[2]

[1]*Instituto de Física Aplicada, Consejo Superior de Investigaciones Científicas, Serrano 144—28006 Madrid, Spain*

[2]*Syscom Laboratory, Ecole Nationale d'Ingénieurs de Tunis, 37, Le Belvédère 1002 Tunis, Tunisia*

Chaos and Cryptography

From Chaos...



Confusion ← Topological mixing ↔ Sensitivity to initial conditions and control parameter → Diffusion

... to chaos-based cryptography

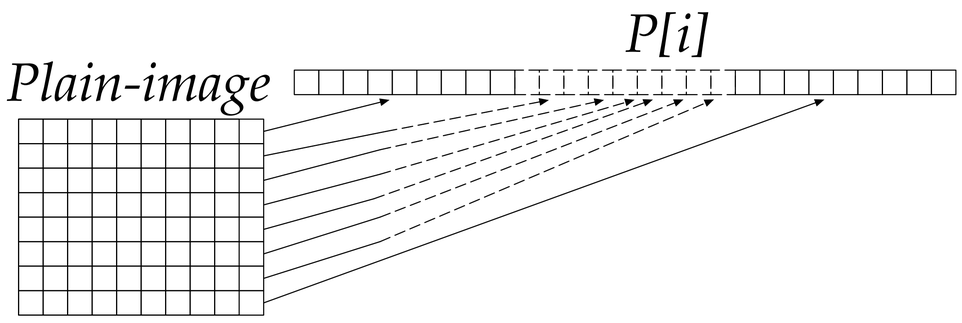
Encryption architecture

- Take benefit of chaos
- Do not show enough information to reconstruct the dynamics of the underlying chaotic system

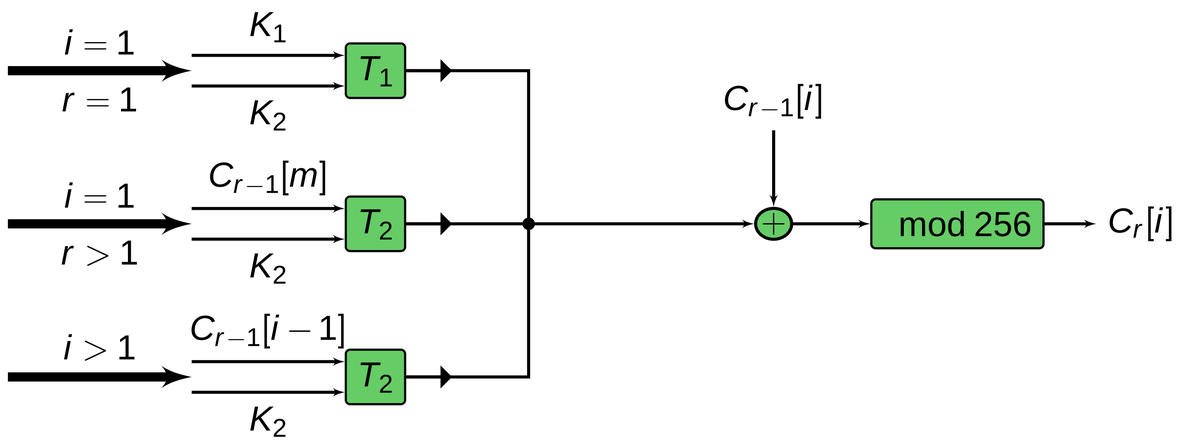
Chaotic system: $f(x, \lambda)$

- Uniform probability distribution
- Easy selection of control parameter values
- Simple: low cost implementation

Our proposal



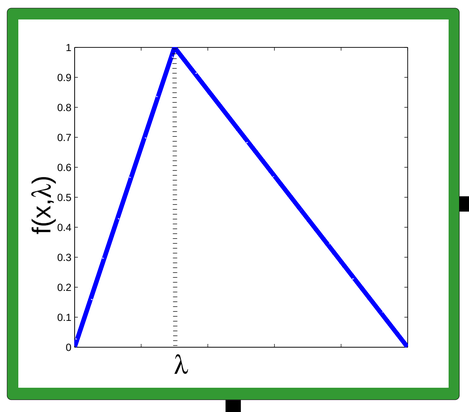
- P contains m elements
- $C_0[i] = P[i]$
- R encryption rounds $\Rightarrow r = 1,\ldots,R \Rightarrow i = 1,\ldots,m \Rightarrow C_R \equiv cipher - image$
- Encryption similar to decryption but starting from the last pixel



$x, y \xrightarrow{T_1} z = T_1(x,y) = h(f(x,y))$

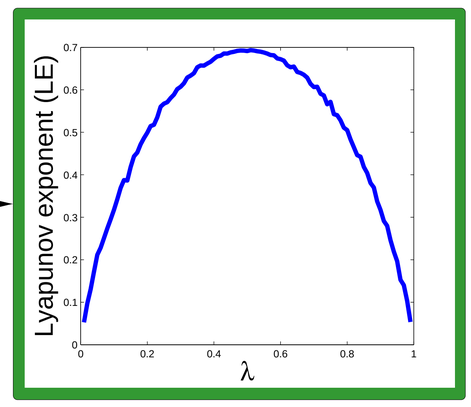
$x, y \xrightarrow{T_2} z = T_2(x,y) = h(f(g(x),y))$

Our selection: the skew tent map



Always chaotic

$LE(\lambda) > 0 \ \forall\lambda$

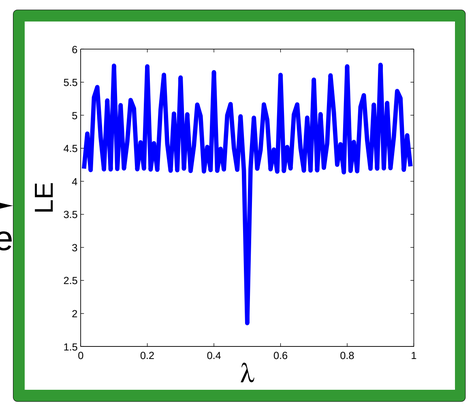


Discretization

$h(x,\lambda) = 2^{33} \cdot f(x,\lambda) \mod 256$

↑ LE

↓ encryption time



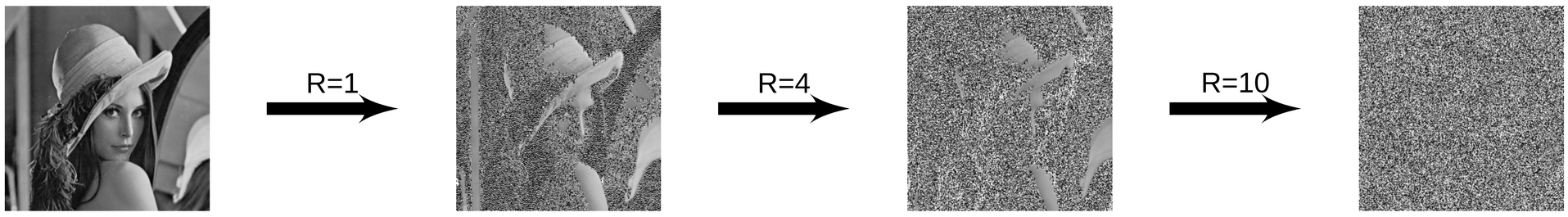
Mapping into the phase space

$g(x) = \frac{2 \cdot x + 1}{512}$

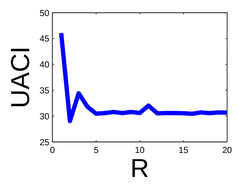
Secret key

$K = (K_1, K_2)$ → K_1 = Initial condition= $x_0 \in (0,1)$ → $K_2 = \lambda \in (0,1)$

Simulations and results



$$UACI = \frac{1}{m}\left(\sum_{i=1}^{m} \frac{|P(i) - C_R(i)|}{255}\right) \times 100$$



$$D(i) = \begin{cases} 0 \; if \; P(i) = C_R(i) \\ 1 \; if \; P(i) \neq C_R(i) \end{cases} \Rightarrow NPCR = \frac{\sum_{i=1}^{m} D(i)}{m} \times 100$$