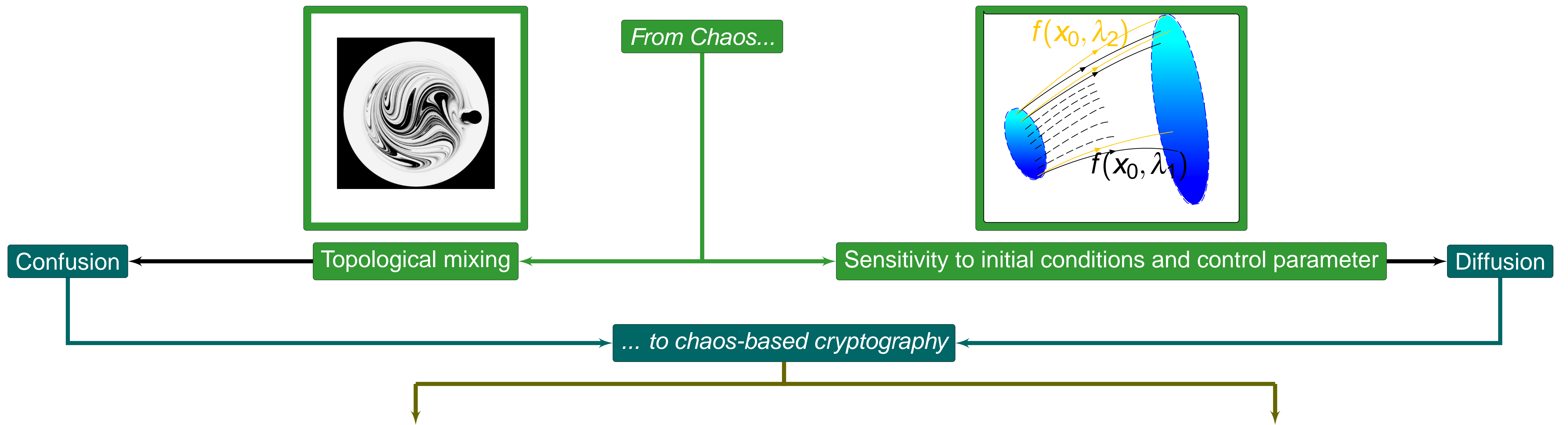


Chaos and Cryptography



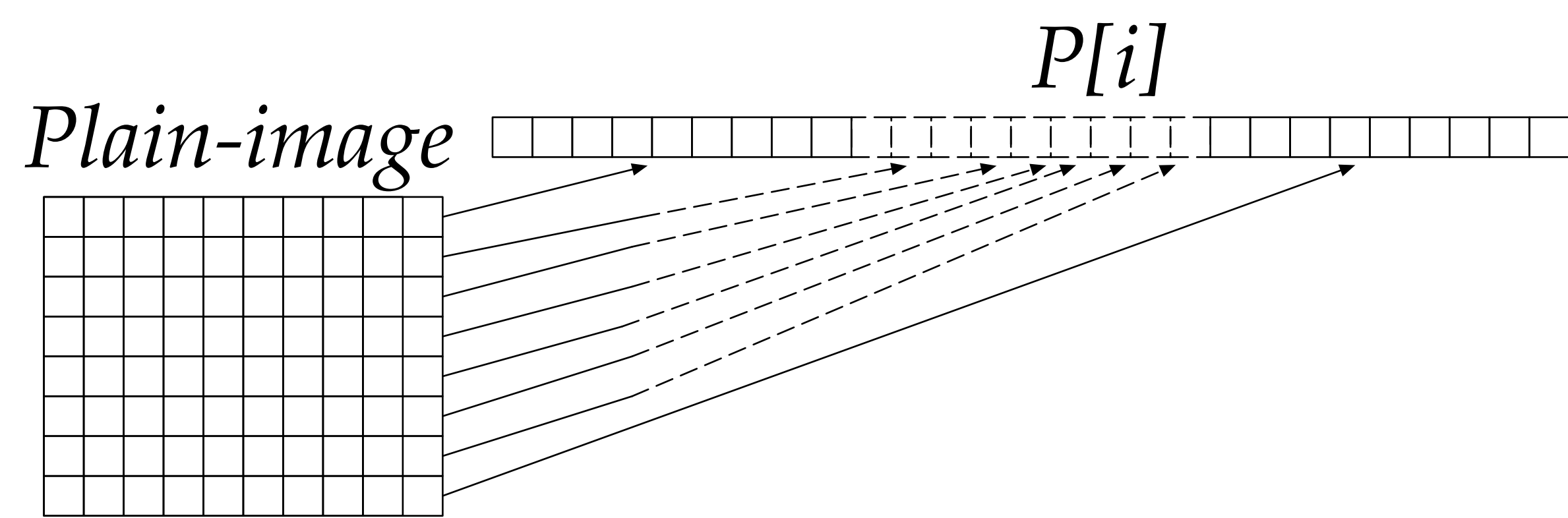
Encryption architecture

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

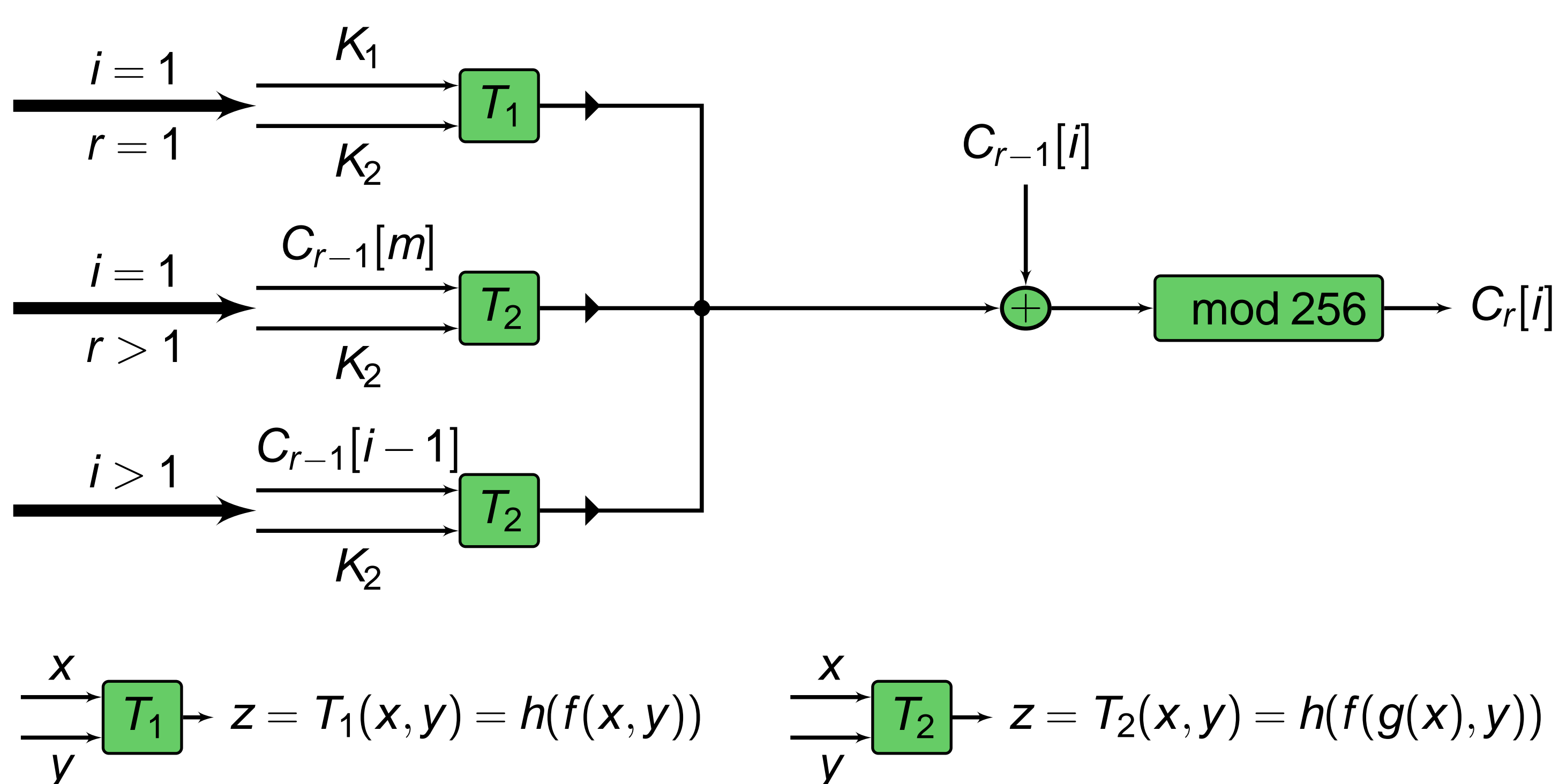
Chaotic system: $f(x, \lambda)$

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

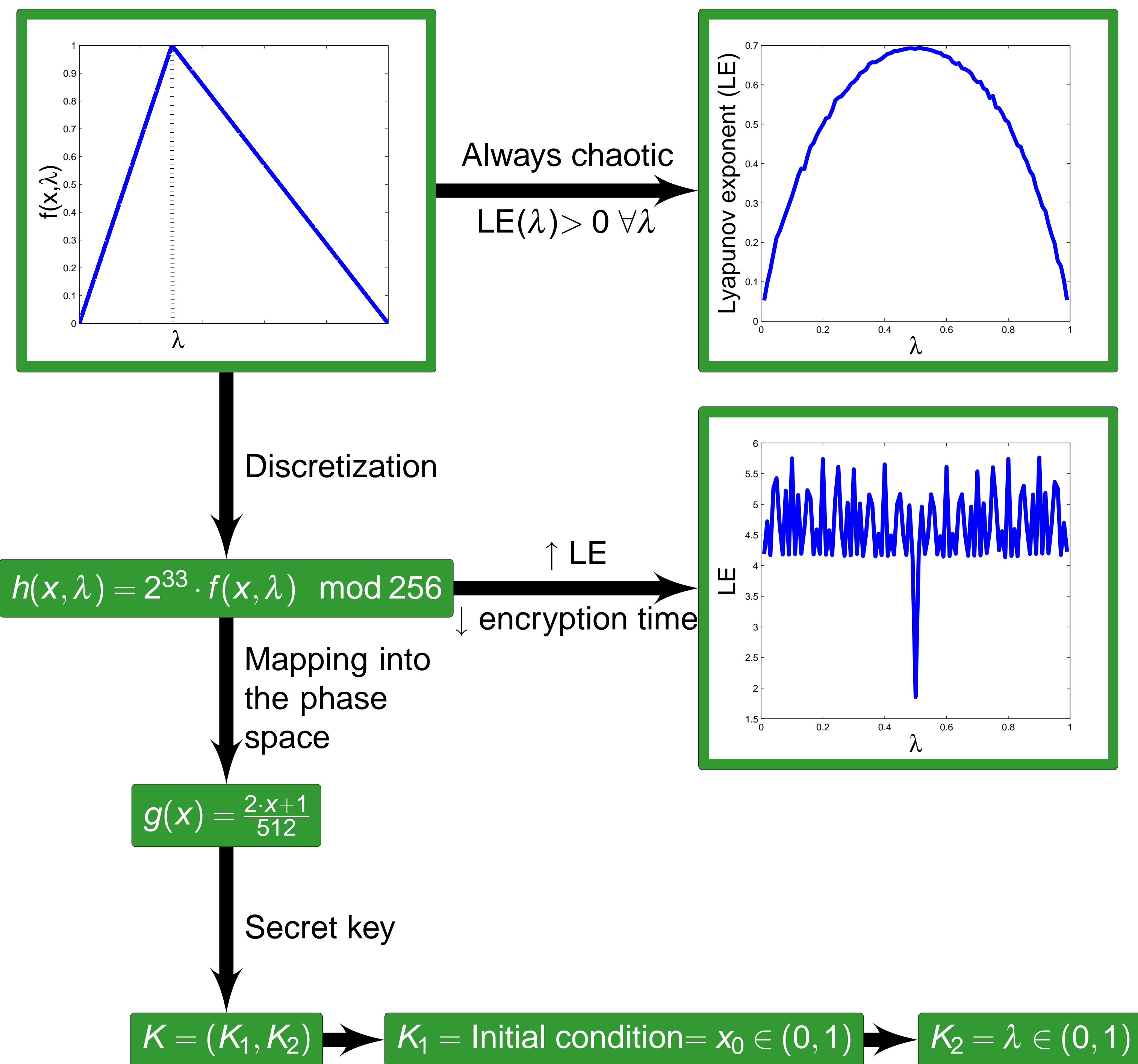
Our proposal



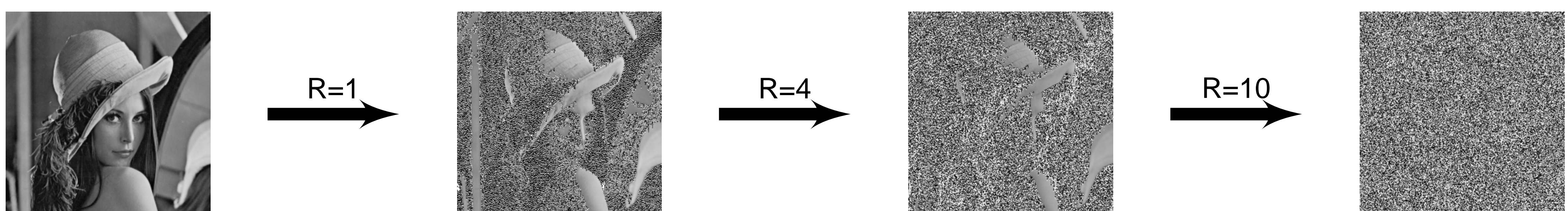
- P contains m elements
- $C_0[i] = P[i]$
- R encryption rounds $\Rightarrow r = 1, \dots, R \Rightarrow i = 1, \dots, m \Rightarrow C_R \equiv \text{cipher} - \text{image}$
- Encryption similar to decryption but starting from the last pixel



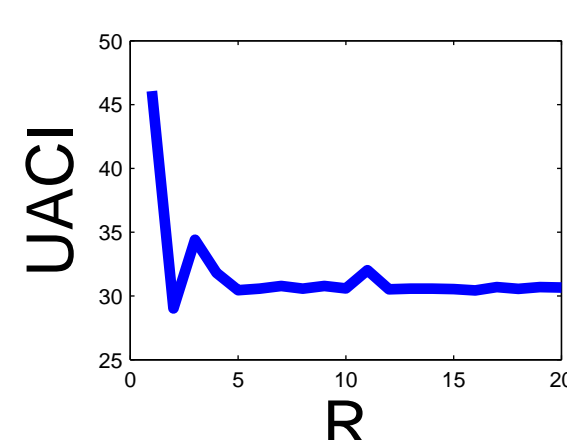
Our selection: the skew tent map



Simulations and results



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



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

