Chaos based cryptography

Benson Muite and Gelo Tabia

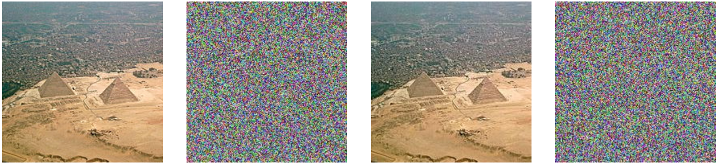
benson.muite@ut.ee and gelo.tabia@ut.ee

4 June 2016

Outline

- Introduction to encryption
- Reversible dynamical systems
- Criticisms from cryptographers
- A possible generic framework
- Conclusions and further work

Some pictures



(a) Original picture of pyramids

(b) Encrypted picture of pyramids

(c) Decrypted picture of pyramids

(d) Decrypted picture of pyramids with perturbation of values of one pixel in encrypted data

Figure: Encryption of a 200 × 200 pixel picture of a pyramid.

Introduction to encryption I

- An encryption algorithm takes information processes it so to produce an output that makes it difficult to determine original data
- For each encryption algorithm, there is a decryption which returns the original data

Introduction to encryption II

- Notions of security
  - Brute force decryption difficult
  - Cannot use linearity to determine mapping from a small subset of inputs and outputs
  - If given the algorithm, knowing multiple inputs and outputs does not allow you to easily determine encryption parameters

Introduction to encryption III

- Good encryption algorithms have the properties that:
    - Nearby inputs are mapped to very different outputs
    - A slight change in an output makes returned data very different than the input
    - Low computational cost
    - Nonlinearity to ensure that one cannot determine map parameters simply from knowing several inputs and their corresponding outputs

Introduction to encryption IV

- The Advanced Encryption Standard
  1. a value change at each location based on composition with the key
  2. a value change at each location based on using a lookup table
  3. a permutation of values within rows and columns.

Reversible dynamical systems

- Provide a simple means to obtain a cryptographic scheme
- Run system forward in time to encrypt
- Run system backward in time to decrypt

Criticisms from cryptographers

- Schemes are to complicated
- Schemes are slow
- Schemes suffer from rounding errors
- Schemes are difficult to analyze

A possible generic framework

- Encryption
  - Shuffle information between locations - use invertible incompressible mapping
  - Change value of pixels - use invertible mapping
  - Mix values at related locations - use reversible discretization of reversible in time partial differential equation
- Decryption
  - Unmix values at related locations
  - Change value of pixels
  - Shuffle information

Simple Example

- Use reversible chaotic 2 dimensional dynamical systems to "mix" pixels in an image. To unmix, reverse the dynamical system.
- Example considered here:
  - Shuffle positions using Arnold Cat map
  - Mix using Schrödinger equation
  - Shuffle values using Hénon map

Simple Example: Arnold Cat Map

- Shuffle the locations of pixels in a square ($N \times N$) - use invertible incompressible mapping
- $$\begin{bmatrix} x^{n+1} \\ y^{n+1} \end{bmatrix} = A^n \begin{bmatrix} x^n \\ y^n \end{bmatrix} \mod N, \qquad A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}.$$

Simple Example: Discretized Schrödinger Equation 1

- $$\mathbf{i}u_t = \mu u|u|^2 + \Delta u.$$
- Need to discretize so that floating point errors are not important
- Need to discretize to allow for reversible dynamical system

Simple Example: Discretized Schrödinger Equation 2

- $$\mathbf{i}\frac{u_i^{n+1} - u_i^{n-1}}{2\delta t} = \left|u_i^n\right|^2 u^n + \frac{u_{i+1}^n - 2u_i^n + u_{i-1}^n}{(\delta x)^2}.$$
- Map integers to integers, let $\delta t = \frac{1}{2}$ and $\delta x = 1$
- Forward scheme

$$u_i^{n+1} = u_i^{n-1} - \mathbf{i}\left(\left|u_i^n\right|^2 u_i^n + u_{i+1}^n - 2u_i^n + u_{i-1}^n\right),$$

- Backward scheme

$$u_i^{n+1} = u_i^{n-1} + \mathbf{i}\left(\left|u_i^n\right|^2 u_i^n + u_{i+1}^n - 2u_i^n + u_{i-1}^n\right),$$

Simple Example: Discretized Schrödinger Equation 3

- $$\mathbf{i}\frac{u_i^{n+1}-u_i^{n-1}}{2\delta t} = \left|u_i^n\right|^2 u^n + \frac{u_{i+1}^n - 2u_i^n + u_{i-1}^n}{(\delta x)^2}.$$
- Use modular arithmetic so no overflow errors
- Forward scheme

$$u_{i,j}^{n+1} = \text{mod}\left[u_{i,j}^{n-1} - \right.$$
$$\left. \mathbf{i}\left(\left|u_{i,j}^n\right|^2 u_{i,j}^n + u_{i+1,j}^n + u_{i,j+1}^n - 4u_{i,j}^n + u_{i-1,j}^n + u_{i,j-1}^n\right), M\right],$$

- Backward scheme

$$u_{i,j}^{n+1} = \text{mod}\left[u_{i,j}^{n-1} + \right.$$
$$\left. \mathbf{i}\left(\left|u_{i,j}^n\right|^2 u_{i,j}^n + u_{i+1,j}^n + u_{i,j+1}^n - 4u_{i,j}^n + u_{i-1,j}^n + u_{i,j-1}^n\right), M\right],$$

Simple Example: Hénon map

- Forward

$$x_{n+1} = \text{mod}\left[y_n + 1 - ax_n^2, p\right], \quad y_{n+1} = x_n$$

- Backward

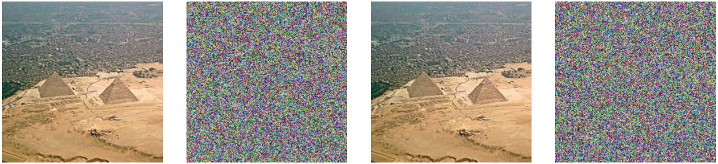
$$x_{n+1} = y_n, \quad y_{n+1} = \text{mod}\left[x_n - 1 + ay_n^2, p\right].$$

- Choose $a > 1$, a an integer that is not a square of integers to ensure there are no fixed points

Possible key parameters

- Adding a background image and how this is chosen
- Number of iterations of Arnold Cat Map
- Number of time steps for Schrödinger equation
- Size of time steps for Schrödinger equation
- Size of coefficient for nonlinear term in the Schrödinger equation
- Power of nonlinear term in the Schrödinger equation
- Modulo operation to perform for discrete Schrödinger equation at each step
- Number of iterations for Hénon map
- Parameter modulo operation to perform for Hénon map at each step
- Alternative methods for composing the three different maps

Some pictures



(a) Original picture of pyramids

(b) Encrypted picture of pyramids

(c) Decrypted picture of pyramids

(d) Decrypted picture of pyramids with perturbation of values of one pixel in encrypted data

Figure: Encryption of a 200 × 200 pixel picture of a pyramid.

Conclusions and further work

- Introduced a scheme based on reversible chaotic maps and discretized reversible partial differential equations
- Scheme shares some characteristics with typical chaotic ciphers, such as the Advanced Encryption Standard
- Operation count of scheme is higher than of typical cryptographic schemes, however will attempt to get it to run fast enough to be used in applications
- Can one apply methods used in understanding mixing for chaotic dynamical systems to understand strength of scheme?
- Computational power that gives fast enough results may allow schemes where one can prove something to be useful
- Determine security of scheme - most orbits have very long period

References

- Balakrishnan, S. “Dispersive quantization”
- Barlas, G. “Multicore and GPU programming: An integrated approach” Morgan Kaufmann (2015)
- Bruin, R. “Giza Pyramids” Wikimedia commons (2011) `https://commons.wikimedia.org/wiki/File:Giza-pyramids.JPG`
- Chen, G., Mao, Y. and Chui, C.K. “A symmetric image encryption scheme based on 3D chaotic cat maps” Chaos, Solitons and Fractals **21**, 749-761 (2004)

References

- Daemen, J. and Rijmen, V. “Specification for the Advanced Encryption Standard (AES)” Federal Information Processing Standards Publication 197 (2001)
- Goldreich, O. “Foundations of Cryptography II” Cambridge University Press (2004)
- Hénon, M. “Numerical study of quadratic area-preserving mappings” Quarterly of Applied Mathematics **27**(3), 291-312 (1969)
- Henricksen, M. “A critique of some Chaotic-Map and Cellular Automata-Based Stream Ciphers” Advances in Computer Science - ASIAN 2009. Information Security and Privacy, LNCS **5913**, 69-78 (2009)
- Muite, B.K. and Tabia, G.N. In preparation

Acknowledgements

European Union
Regional Development Fund

Investing in your future

EXCS
ESTONIAN COMPUTING