Chaos-based Image Encryption Using an AONT Mode of Operation

Andrius Rickus, Eckhard Pfluegel, Nigel Atkins
School of CIS, Faculty of SEC
Kingston University

Cyber Security 2015

C-MRiC.ORG®
Centre for Multidisciplinary Research, Innovation and Collaboration

Kingston University London

Motivation

- Encryption: popular cryptographic tool to establish data confidentiality
- Sensitive data in the form of images is becoming increasingly prevalent in various applications:
  - Biometric data
  - Medical images
- Images have particular characteristics which might make encryption more challenging
- Chaos-based encryption has been traditionally applied to images and offers new perspectives and solutions

Research Contributions

- We design a novel image encryption scheme
  - Use chaos-based encryption employing chaotic maps
  - Combine this with an AONT mode of operation
- We evaluate an implementation of our scheme
  - Implementation in Matlab
  - Show that AONT gives only little computational overhead

Chaos-based Image-Encryption

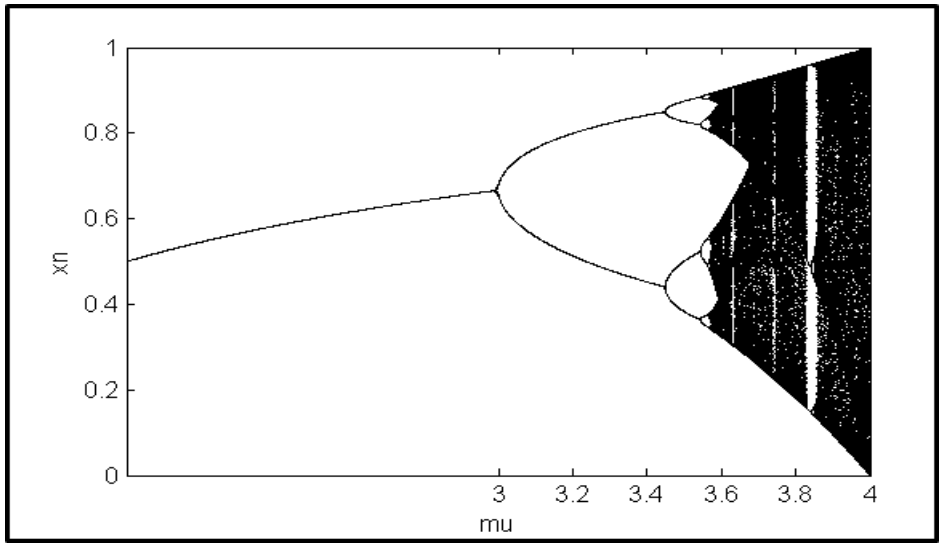
- Based on using chaotic maps as building blocks for encryption primitives
- This implements analytic approach in contrast to algebraic
- Popular techniques:
  - Substitution (stream) cipher: logistic map
  - Transposition cipher: Baker/Cat map
- Main challenge: overcome slow arithmetic

Logistic Map

- Use logistic equation

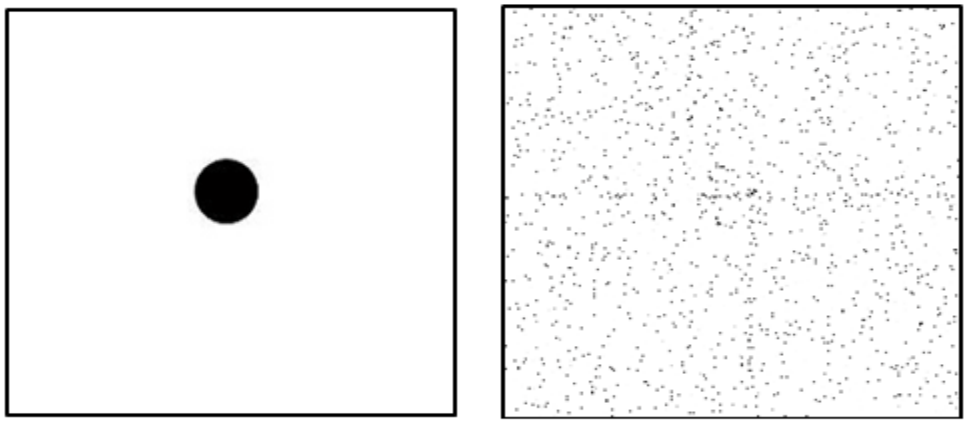
$$x_{n+1} = r x_n (1 - x_n)$$

with suitable parameters $3.57 < r < 4$ and $x_0 \in [0..1]$ as a pseudo-random number generator

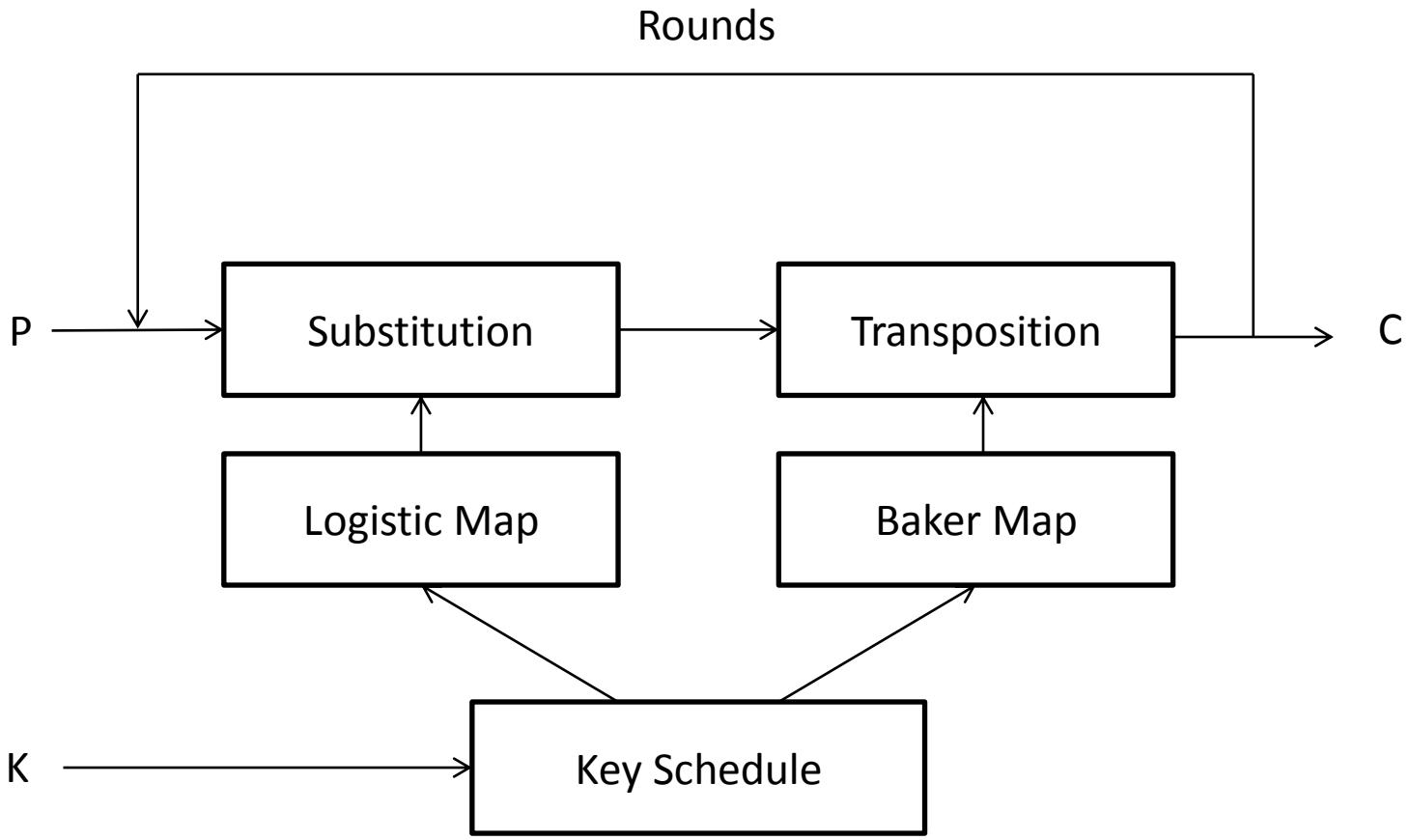


Baker Map

- This is a chaotic map from unit square to itself
- Discrete 2-D Baker map implements a transposition cipher with good diffusion properties



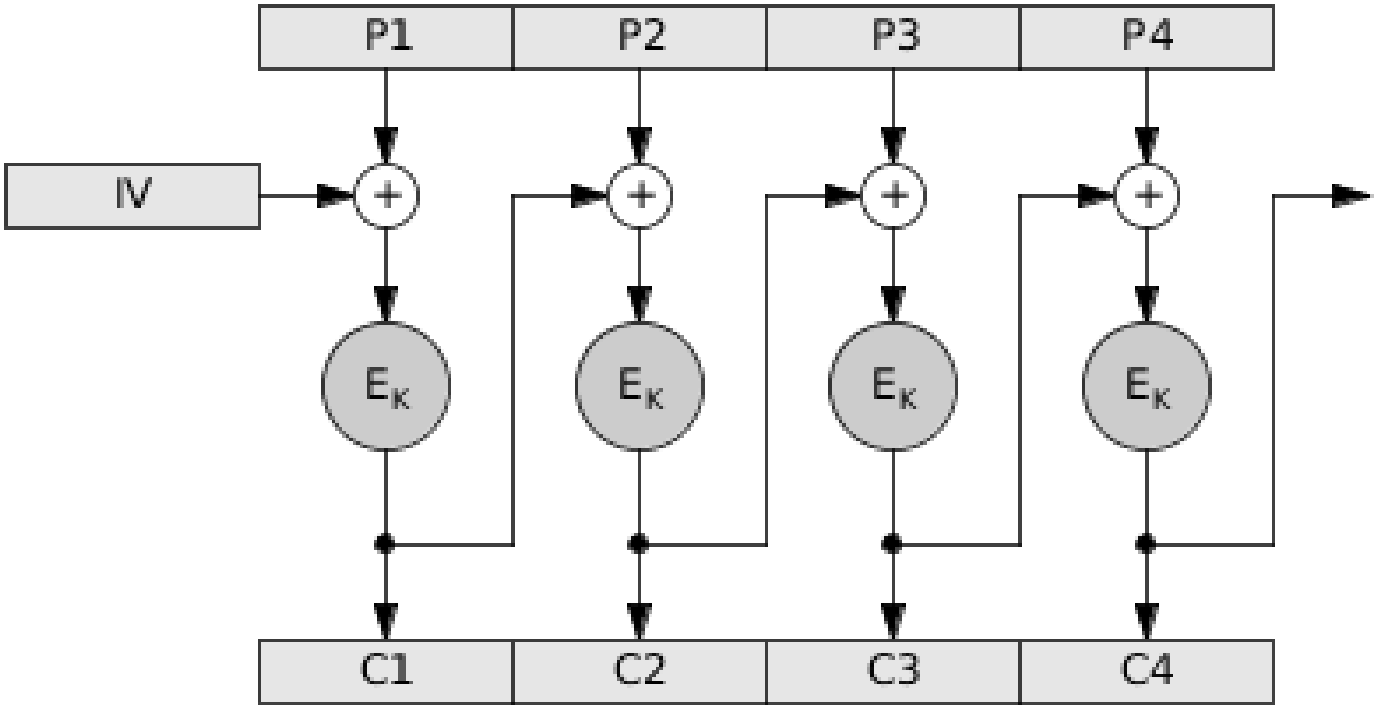
Encryption Algorithm Design



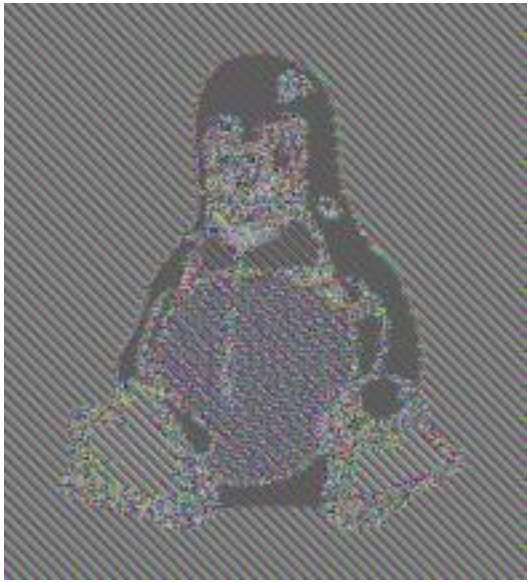
Encryption Modes of Operation

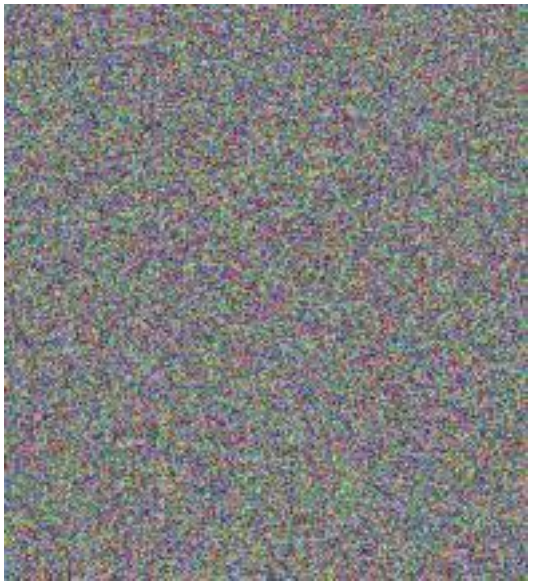
- Encryption mode of operation prescribes how to implement encryption across blocks
- Popular modes: ECB, CBC, CTR
- Drawbacks:
  - Poor diffusion (ECB)
  - Partially vulnerable to bit-flipping attack (CBC)
  - Separable (all modes)

CBC Mode



CBC vs ECB Mode

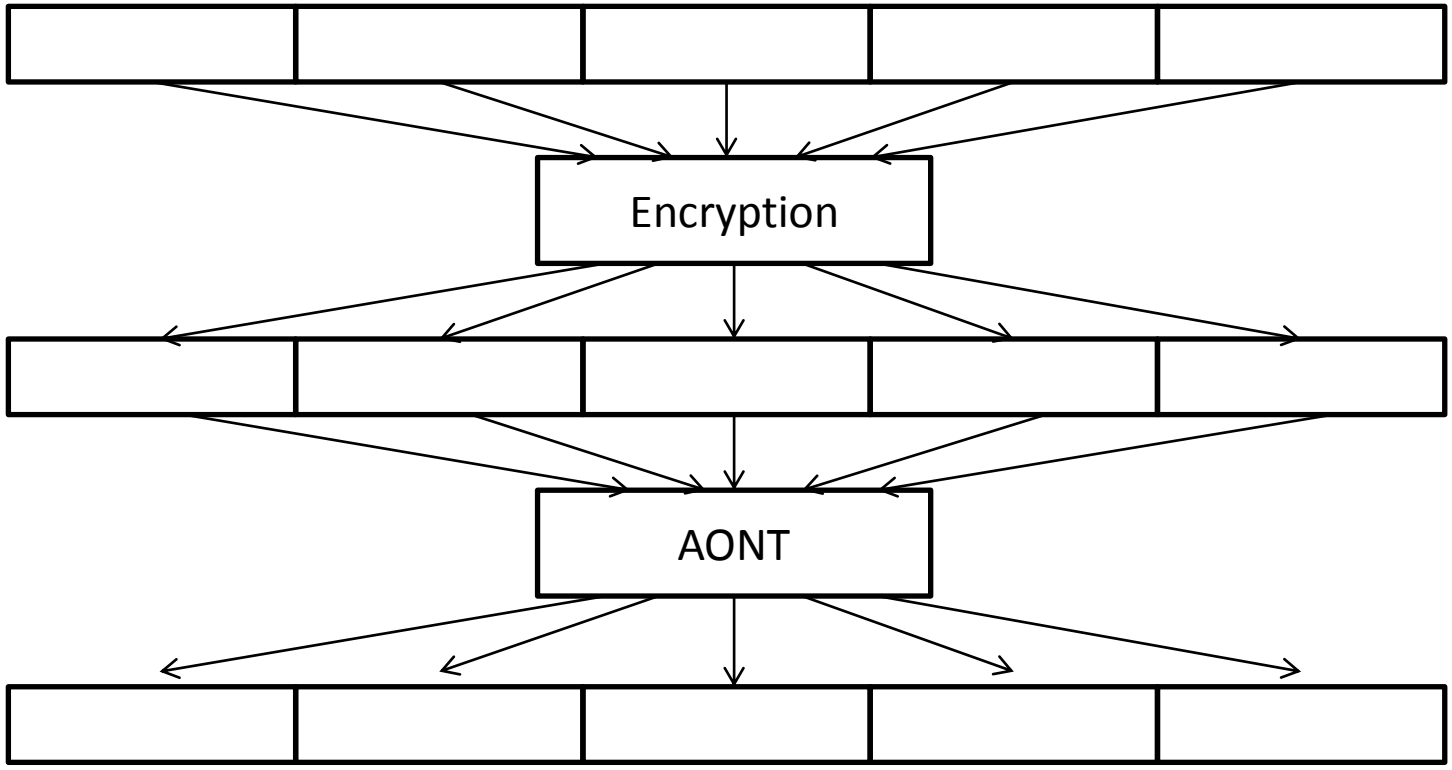




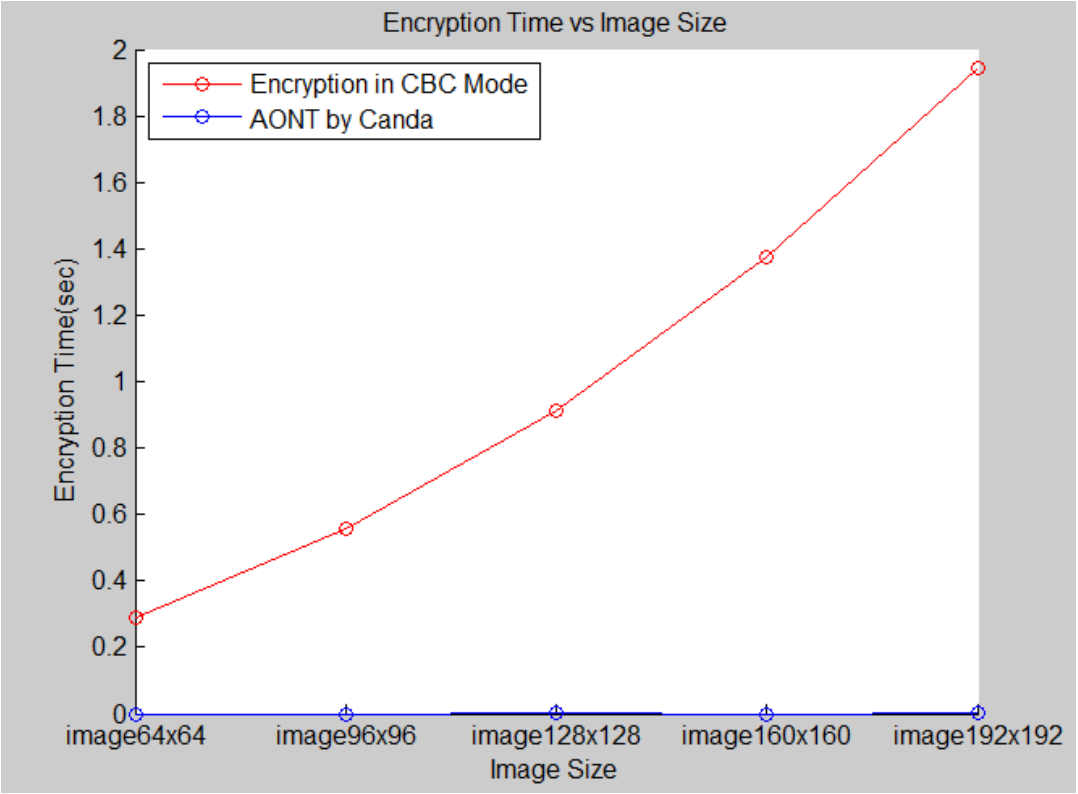
AONT Mode

- Fundamental property: any plaintext block depends on *all* cipher blocks
- Implemented through appropriate *all-or-nothing transform* (AONT)
  - [Rivest]: first design of AONT using XOR function, as pre-processor to AES
  - [Canda]: use of linear AONT as post-processor for AES in CBC mode
  - Our work: inspired by Canda, but using chaotic encryption

Final Architecture



Evaluation


Encryption Time vs Image Size
Encryption in CBC Mode
AONT by Canda
Encryption Time(sec)
2
1.8
1.6
1.4
1.2
1
0.8
0.6
0.4
0.2
0
image64x64
image96x96
image128x128
image160x160
image192x192
Image Size

Conclusion

- We have focused on encryption mode of operation, in the context of chaos-based encryption
- Next steps for future research:
  - Find alternative design for chaos-based block cipher
  - Evaluate security (e.g. using NIST test suite)
  - Improve efficiency