STORAGE DEVELOPER CONFERENCE
SDC22
Fremont, CA
September 12-15, 2022
BY Developers FOR Developers
A SNIA Event

Power of Chaos: Long-term Security for Post-quantum Era

Rahul Vishwakarma
Graduate Student
California State University, Long Beach
rahuldeo.vishwakarma01@student.csulb.edu

Dr. Amin Rezaei
Assistant Professor
California State University, Long Beach
amin.rezaei@csulb.edu

Dr. Ava Hedayatipour
Assistant Professor
California State University, Long Beach
ava.hedayatipour@csulb.edu

CALIFORNIA STATE UNIVERSITY LONG BEACH

Agenda

- Post-quantum era
- Chaos cryptography
- Conclusion

Post Quantum Era

Risks for classical cryptography

Asymmetric cryptography

- Security foundations
  - Integer factorization
  - Discrete logarithms

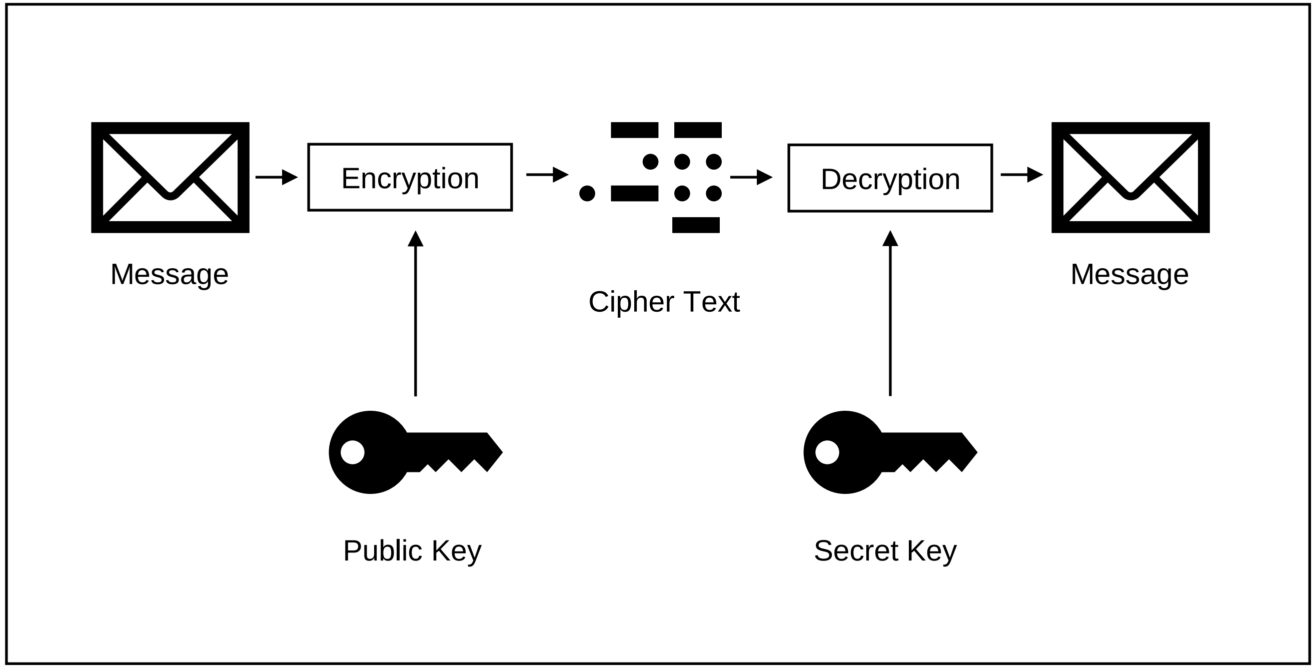
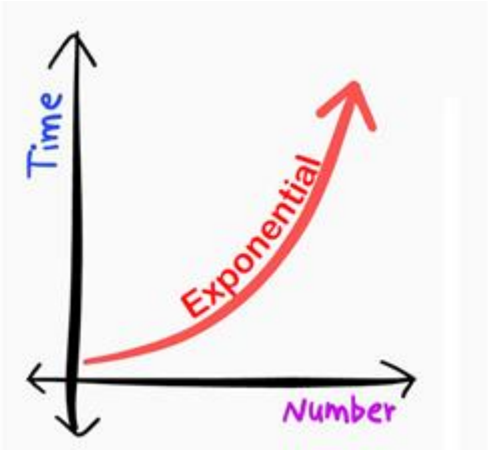


Figure 1: Asymmetric cryptography

Post-quantum era

- Quantum computers
  - Qubits
    - Superimposition
    - Entanglement
- Shor's algorithms
  - Impact on classical cryptography
    - RSA scheme
    - Finite Field Diffie-Hellman key exchange
    - Elliptic Curve Diffie-Hellman key exchange



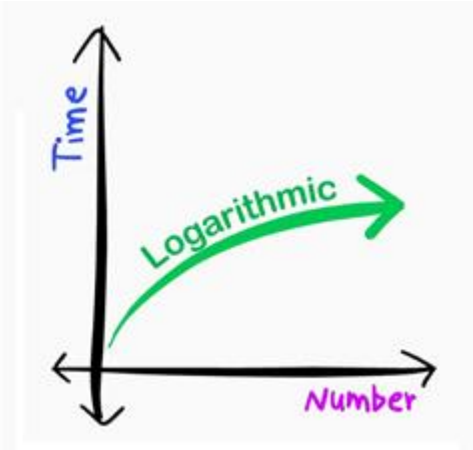


Figure 2: Classical Vs Quantum computers to break cryptosystem

STORAGE DEVELOPER CONFERENCE

Quantum safe algorithms

- Lattice
- Code
- Hash
- Non-commutative
- Multivariate
- Isogeny

Academics and Industry

- PyCrypto
- European Telecommunications Standards Institute (ETSI)
- Institute of Quantum Computing

Where we need quantum safe cryptography?

- Medical records
  - 5 – 100 years
- Implantable wearable devices
  - Biomedical devices
- Financial institutions
  - Tax
- Communication

Chaos-Based Cryptography

Chaos

- Properties
  - Deterministic
    - Mathematical model
  - Nonlinear
    - Logistic map
  - Sensitive dependence
    - Butterfly effect

Chaos – Deterministic

- Mathematical model
  - Discrete equations
    - Logistic map
  - Differential equations
    - Lorenz system

Chaos – Nonlinear

- Logistic Map

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

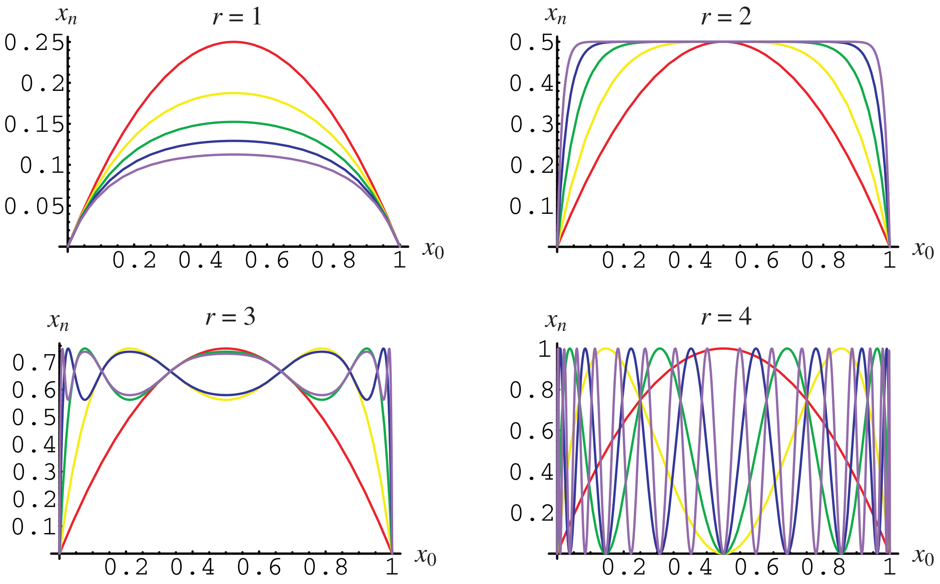


Figure 3: Plotting logistic map for different values of r

Chaos – Sensitive dependence

- Butterfly effect

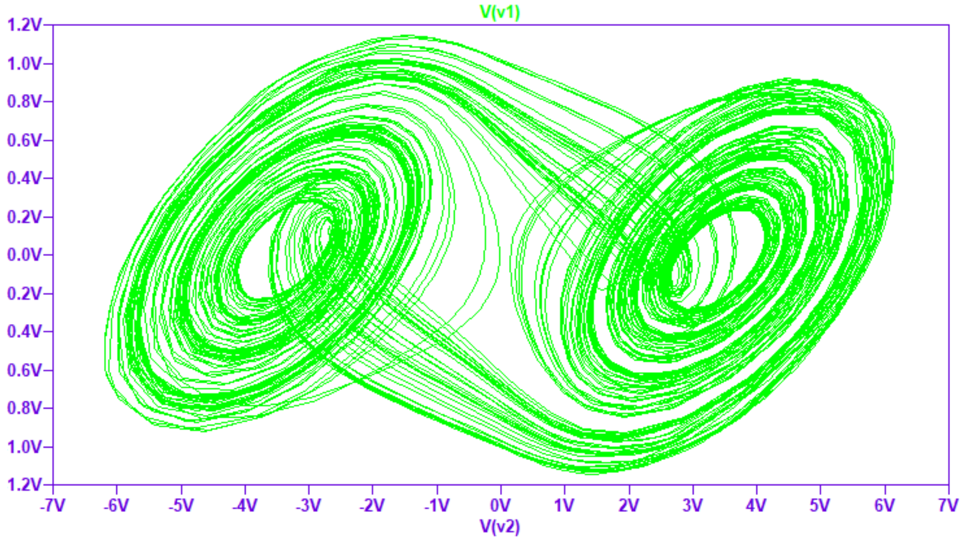


Figure 4: Double scroll attractor for Chau chaotic equations

0.1	0.101
0.3465	0.34957615
0.871785338	0.875384762
0.430336302	0.419982181
0.943815831	0.937849022
0.204155905	0.2244097
10.62553365	0.670092448
0.901829019	0.851113953
10.34085374	0.48786812
10.864989	0.961933347
0.449614656	0.140977693
0.952726071	0.466246485
0.173400554	0.958113696
0.551831287	0.15450759
0.952157043	0.50294473

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

Cryptographic algorithms and chaotic system

Cryptographic algorithms	Chaotic Systems
Finite set of integers	(sub)set of real numbers
Algebraic methods	Analytic method
Rounds	Iterations
Key (Boolean) – Discrete keyspace	Parameters (real) – Continuous keyspace
Diffusion	Sensitivity to change in initial condition
Security and performance	?

Chaotic system architecture

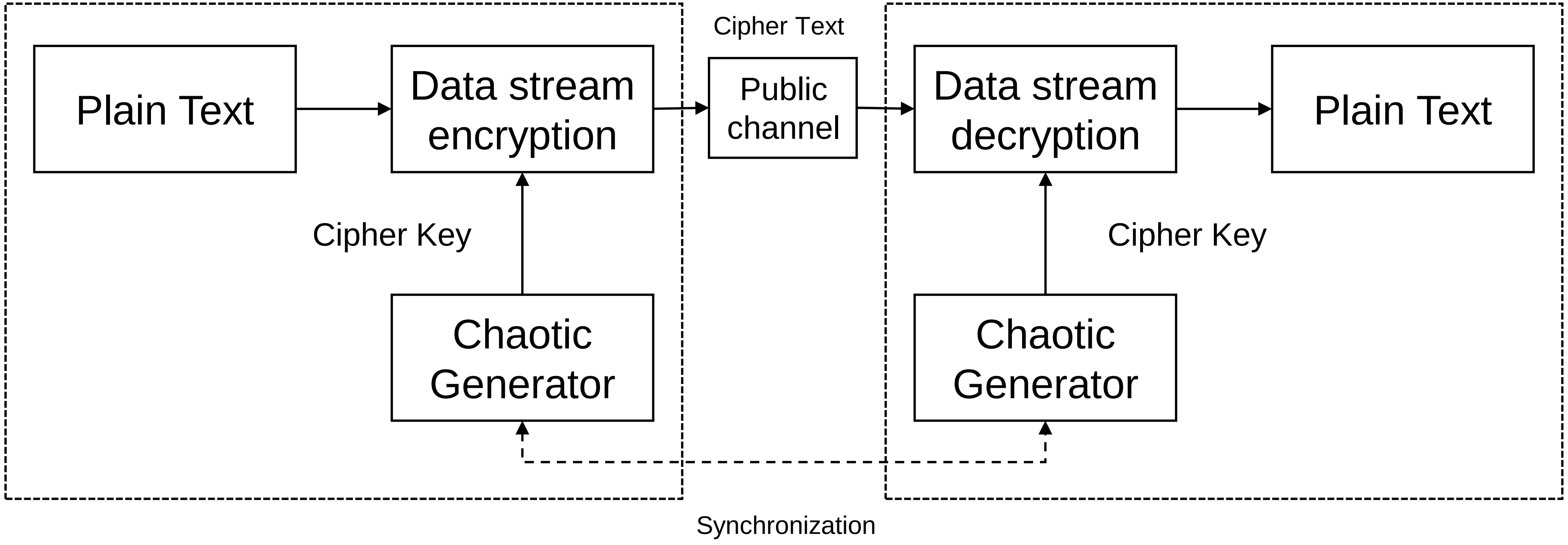


Figure 5: High level architecture of chaotic cryptography

Chua chaotic circuit

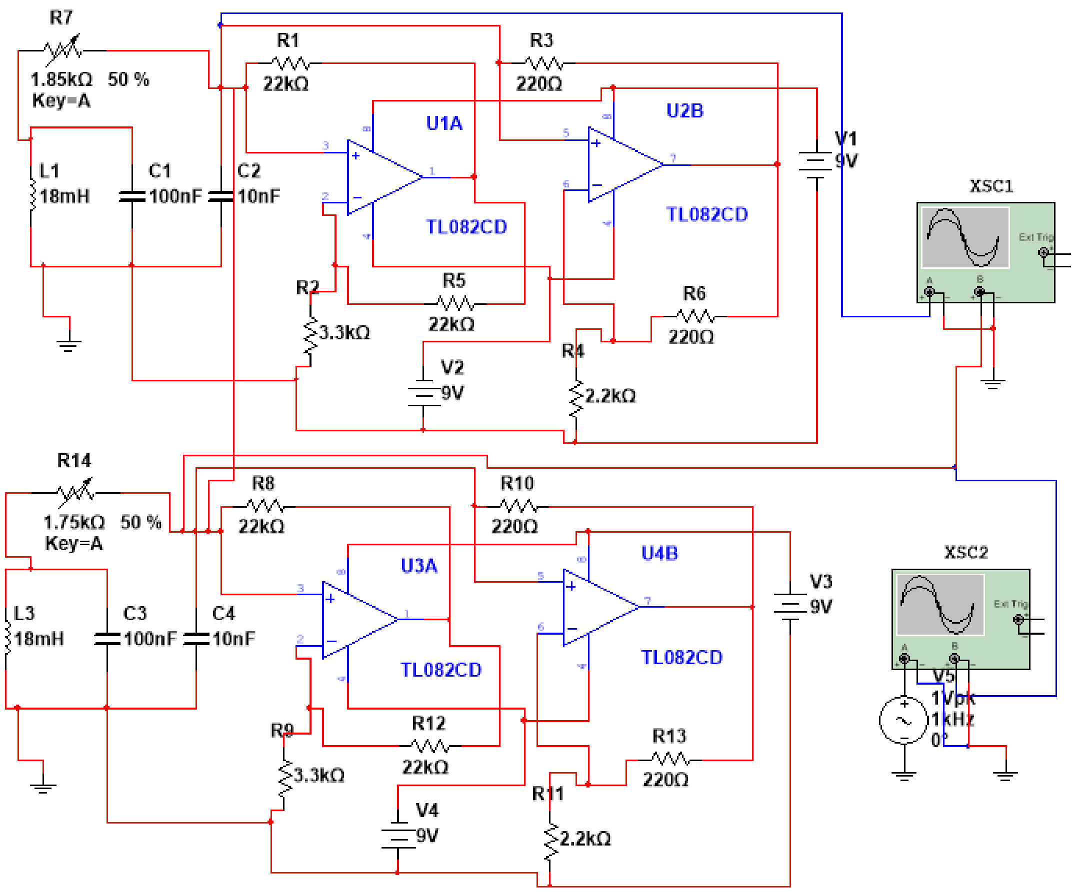


Figure 6: Circuit realization of Chau chaotic circuit

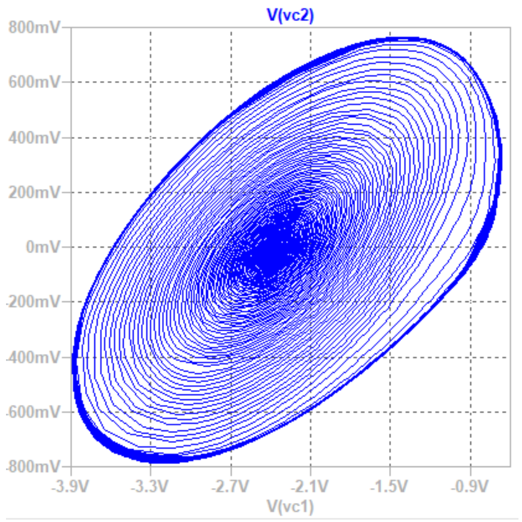


Figure 7: Single scroll attractor

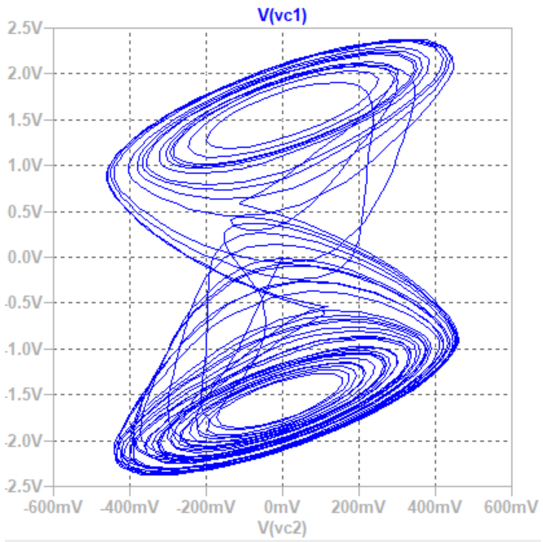


Figure 8: Double scroll attractor

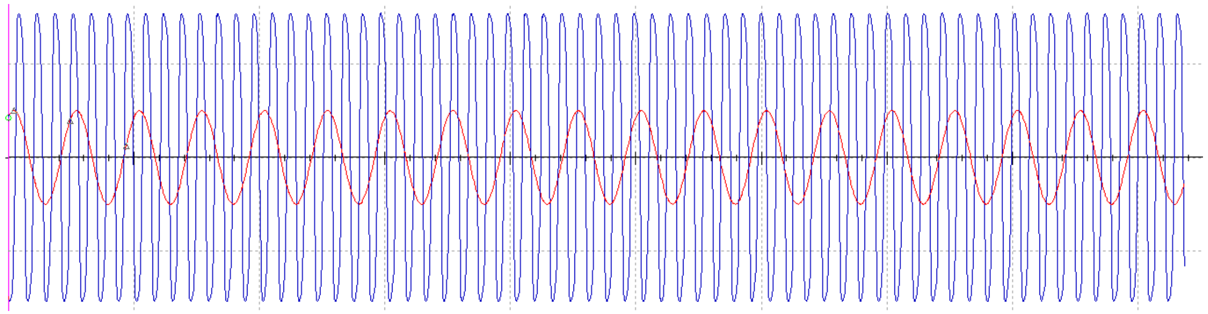


Figure 9: Plain text and encrypted information with Chaos

STORAGE DEVELOPER CONFERENCE

Chua chaotic circuit

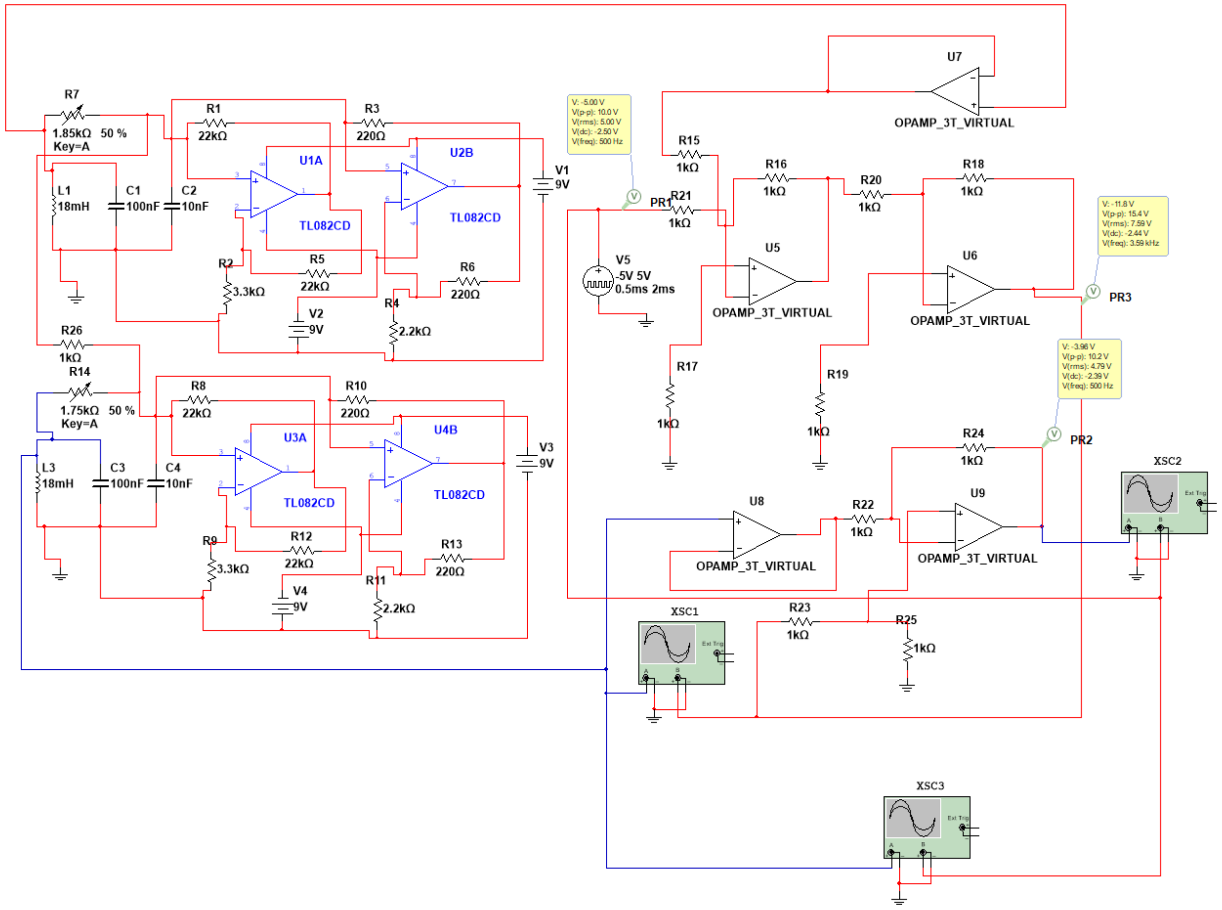


Figure 10: Circuit realization of Chau chaotic circuit with different initial values

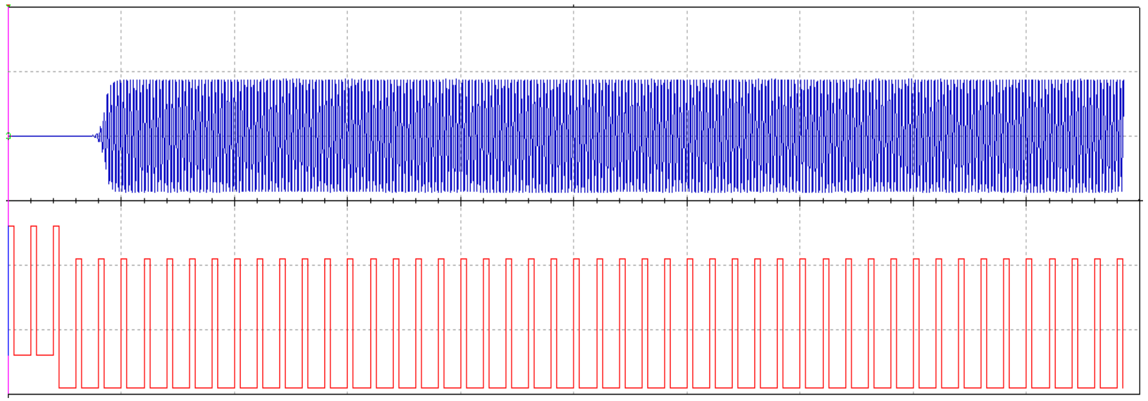


Figure 11: Actual message in red and encrypted message in blue

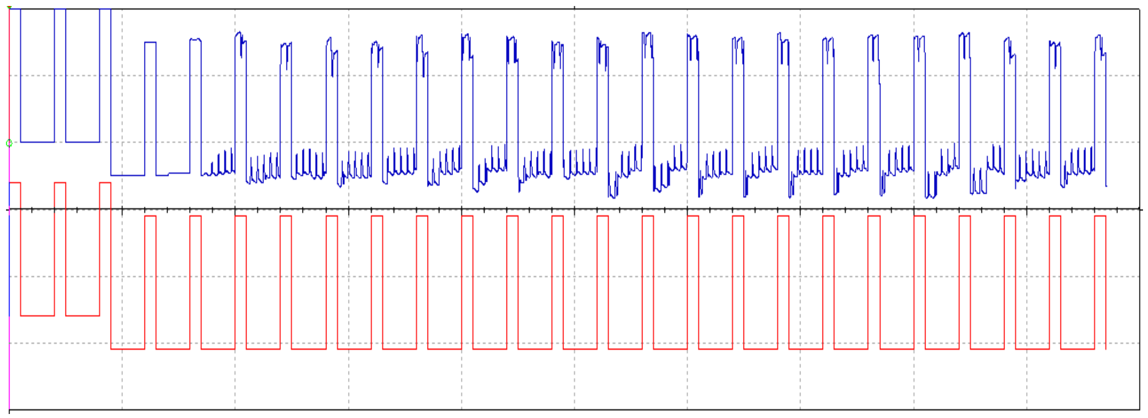


Figure 12: Actual message in red and decrypted message in blue

Implementation challenges

- Definition of the key leading to non-chaotic behavior
- Nonuniform probability distribution function
- Return map reconstruction
- Low sensitivity to secret key
- Erosion of computational efficiency due to the structural complexity

Design rule for chaos-based cryptography

- Exhaustive and rigorous definition of key and the keyspace
- Selection of chaotic maps with high sensitivity to control parameter mismatch
- Analysis of the performance of chaotic orbits as source of entropy
- Resistance to application-specific attacks
- Resistance to classical attacks

Industrial Adoption

National Institute of Standards and Technology (NIST)

- Lattice problems and hash functions
  - Public-key-encryption (1)
  - Digital signatures (3)

- Post-quantum Cryptography VPN, Microsoft
- PICNIC (Digital signature algorithms), Microsoft
- Quantum Safe services: Kyber, IBM
- AWS KMS API endpoints, AWS KMS

Conclusion

Conclusion

- Understanding chaos-based cryptology
- Challenges in implementing post-quantum era cryptography
- No silver bullet for quantum safe algorithms
- Growing industrial adoption
  - Chaos-based cryptography (?)

Please take a moment to rate this session.

Your feedback is important to us.

STORAGE DEVELOPER CONFERENCE

SDC 22