Meeting Results

Mohamed Emary Mohamed Abdelfattah Abdelfattah Zakaria

Shrouk Elsayed Dalia Abdallah Sara Reda

November 29, 2023

1 Encryption Table

1. Code From Repo Or The Code We Already Have
2. Apply hexadecimal to input text before encryption
3. Get Input Text
    1. Encrypt Multiple Files With Different Sizes Of Text
4. Handle Padding
5. **Code** (ask Dr)
6. Add Analysis
7. Try to apply polynomial equations into our algorithm

---

2 Paper

2.1 What Is This Paper About

This paper is about using EEG data from schizophrenic patients to generate true random numbers and create dynamic substitution boxes (S-boxes) for block cipher encryption. Some key points:

- They extract true random bits by calculating differences between EEG readings from multiple schizophrenic patients during a sensory task. These bits pass NIST statistical tests for randomness.
- They use the random bits to generate dynamic S-boxes instead of using algebraic or chaotic approaches. This makes their S-boxes immune to common attacks on those approaches.
- To the authors' knowledge, this is the first research utilizing a psychiatric disorder (the randomness in EEG signals from schizophrenia) to design a cryptographic primitive.
- They develop an image encryption scheme using their dynamic S-boxes along with diffusion layers and show it passes security and statistical tests like differential analysis, histogram analysis etc.

So in summary, it introduces a novel way to harness the randomness inherent in brain signals from schizophrenia to generate dynamic S-boxes resilient against various attacks, with an application to image encryption. The fusion of computing, neuroscience and math to design cryptographic primitives is a key contribution.

2.2 What Is The Aim Of The Research

The main aim of the research is:

1. To propose a methodology to construct the nonlinear component (also known as substitution boxes or S-boxes) for block ciphers using true randomness.

Specifically, the aims are:

2. To generate true random bits by utilizing the inherent randomness in the EEG signals of schizophrenic patients during a sensory task.
3. To use these true random bits for dynamically generating substitution boxes for block ciphers instead of commonly used algebraic and chaotic approaches. This makes the S-boxes immune to known attacks on algebraic and chaotic S-boxes.
4. To design an image encryption scheme using the proposed dynamic confusion components along with diffusion layers and test its security.
5. To open new possibilities of designing cryptographic primitives by fusing computing, neuroscience and mathematics - as this is the first research exploiting the randomness in brain signals from a psychiatric disorder for cryptographic design as per the authors' knowledge.

So in essence, the main aim is to harness the randomness in EEG signals from schizophrenia to construct secure dynamic substitution boxes and use them to build cryptographic applications like image encryption. The novelty lies in utilizing brain signals from a neurological disorder for cryptographic design.

2.3 What Are They Trying To Achieve

Based on the paper, the main things the authors are trying to achieve are:

1. Propose a new methodology to construct substitution boxes (S-boxes). for block ciphers using true randomness rather than algebraic or chaotic approaches.
2. Generate true random bits by exploiting the natural randomness inherent in EEG readings of schizophrenic patients. Assess the randomness using NIST tests.
3. Dynamically generate cryptographic S-boxes using the true random bits. Show these S-boxes are immune to known attacks on algebraic and chaotic S-boxes.
4. Evaluate the security of the proposed S-boxes using standard criteria like nonlinearity, strict avalanche criterion, bit independence criterion etc. Show that the S-boxes pass these criteria.
5. Utilize the proposed S-boxes to build an image encryption scheme using confusion and diffusion layers. Apply security analyses like differential analysis, key space analysis, statistical tests etc. to demonstrate its security.
6. Introduce the novel concept of using randomness in brain signals from a psychiatric disorder (EEG signals from schizophrenia patients) for generating cryptographic primitives.

In summary, they aim to achieve secure, attack-resilient S-boxes and an image encryption scheme using those S-boxes. The main novelty is in harnessing randomness from EEG signals of schizophrenics to generate true random bits and dynamic S-boxes in a previously unexplored way.

2.4 How Will They Acheive That

The authors propose a systematic approach to achieve their aims:

1. Collect EEG readings from 49 schizophrenia patients during a sensory button press task. Extract randomness by calculating differences between EEG readings across electrodes and patients. Fuse the random bits using an algorithm.
2. Assess 1 million extracted random bits using the NIST statistical test suite to demonstrate true randomness.
3. Propose algorithms to generate two-dimensional maps from the random bit vectors and then construct dynamic substitution boxes (S-boxes) of different sizes using these maps.
4. Evaluate security of the generated S-boxes using standard criteria like nonlinearity, Strict Avalanche Criterion, Bit Independence Criterion, Linear Approximation Probability and Differential Approximation Probability.
5. Apply the dynamic S-boxes in developing a symmetric image encryption scheme involving substitution layers based on the proposed S-boxes along with diffusion layers and key addition operations.
6. Perform security evaluation of the image encryption scheme using various analyses like key space analysis, differential analysis (using NPCR and UACI metrics), correlation analysis, entropy analysis and histogram analysis.

So in summary, their systematic methodology involves: data collection > randomness extraction > S-box generation > S-box evaluation > application to image cipher > image cipher security analyses.

This approach lets them rigorously prove the viability of using EEG signals from schizophrenia to construct attack-resilient dynamic S-boxes and use them in a demonstrably secure image cipher, achieving their aims.

2.5 What Is The Coclusion Of The Paper

The main conclusions of the paper are:

1. The inherent randomness in EEG readings of schizophrenic patients undergoing a sensory task provides an excellent source of true randomness that passes stringent NIST statistical tests.
2. The proposed method of using differences in EEG signals across multiple patients and electrodes is effective for extracting robust true random bits.
3. Dynamic and attack-resilient substitution boxes (S-boxes) for block ciphers can be constructed using the true random bits generated from EEG signals.
4. The proposed S-boxes demonstrate strong security performance when evaluated on nonlinearity, strict avalanche criterion, bit independence criterion and other standard criteria.
5. The security analyses of the image encryption scheme devised using the proposed S-boxes proves it can withstand various cryptanalytic attacks.
6. This pioneering research successfully demonstrates the viability of using randomness in brain signals from neurological disorders to design secure cryptographic primitives.

In conclusion, EEG signals in schizophrenia patients provide randomness that can generate dynamic S-boxes to design secure ciphers. More broadly, neurological disorders could provide randomness for future cryptosystems. This opens up an innovative intersection of neuroscience and cryptography.

2.6 Why Schizophrenic Patients And Not Healthy People

The authors chose to use EEG signals from schizophrenic patients rather than healthy people for generating randomness due to some key reasons:

1. Schizophrenia causes altered and irregular neural activities in the brain across various regions. This leads to inherent randomness in the EEG signals of patients.
2. Several symptoms of schizophrenia like delusions, hallucinations, disorganized thinking and behavior stimulate uncertain and unpredictable neural firings.
3. The wide heterogeneity in type and presentation of symptoms amongst patients results in diversity of EEG patterns.
4. No two patients exhibit identical abnormalities in their EEG signals. The variability across patients enhances randomness.
5. Healthy brains have more structured and predictable signal patterns. Schizophrenic brains provide more entropy across spatial regions and symptom dimensions.

In summary, the pathological abnormalities of neural functions in schizophrenia introduce more variability and randomness in EEG signals compared to healthy brain patterns. Leveraging this aspect, the authors could extract randomness from the complex disease processes rather than normal functioning brains. This allowed them to harness maximum entropy and achieve true randomness for cryptographic purposes.