Memristor-Enhanced 1D Logistic Map-Based Random Number Generator for Secure ECG Signal Encryption and Decryption

Nishat Tasnim Hiramony*, Sushmit Hossain*, Himaddri Roy,
Jiacheng Ye, Ting-Hao Hsu, Hongming Zhang, and Wei Wu†

Viterbi School of Engineering, University of Southern California, Los Angeles, California 90089, United States

†wu.w@usc.edu

**These authors contributed equally*

Abstract

Memristors are gaining significant attention as key components for in-memory computation, offering substantial potential in analog circuits due to their adjustability, stochastic behavior, and non-volatility. Their inherent stochastic nature makes them well-suited for random number generators, strengthening security functions in communication systems. Random and pseudorandom number generators are crucial to cryptographic protocols, as they produce unpredictable sequences essential for secure data transmission. In this study, we harness the memristor's fluctuation characteristics to design and implement a memristor-enhanced analog RNG circuit based on a 1D logistic map. The stochastic behavior of memristor amplifies the complexity and unpredictability of the generated sequence, producing random numbers that conventional coding schemes cannot replicate.

The random number sequence generated by our RNG circuit is utilized to encrypt sensitive biomedical data like ECG for telemedicine applications. Drawing upon the stochastic behaviour of memristors, the RNG generates a high-entropy random sequence, being utilized to mask the ECG signal in the frequency domain using the Discrete Cosine Transform (DCT). The DCT coefficients of the ECG signal are perturbed through projecting the RNG sequence onto these components that results in encrypted signals with near-zero correlation ($r < 0.005$) and ultralow Structural Similarity Index ($SSIM < 0.01$), making the encrypted ECG indistinguishable from noise. At the receiver end, the reversible decryption process, enabled by the same RNG-derived sequence, achieves lossless reconstruction of the original ECG signal ($SSIM \approx 1$), preserving its clinical integrity and diagnostic utility. The NIST-compliant RNG thus guarantees cryptographic robustness for practical biomedical data protection and secure transmission.

The results of this study are demonstrated in the Fig.1. where Fig. 1. (a) describes the detailed fabrication process: (i) bottom electrode deposition, (ii) Al_2O_3 layer deposition, (iii) Ta deposition, (iv) top Pt deposition, (b) and (c) show the memristor structure and optical image, (d) displays the memristor I-V characteristics, highlighting its multistate properties, (e) illustrates the fluctuation characteristics of the memristor, (f) shows our analog 1D logistic map-based RNG circuit utilizing the memristor's stochastic nature, (g) presents the uniform histogram of the generated random sequences, (h) displays three different sequences evolving from the same seed, (i) depicts the encrypted ECG signal with -10.38 dB SNR, (i) shows the decrypted ECG signal with 312 dB SNR.

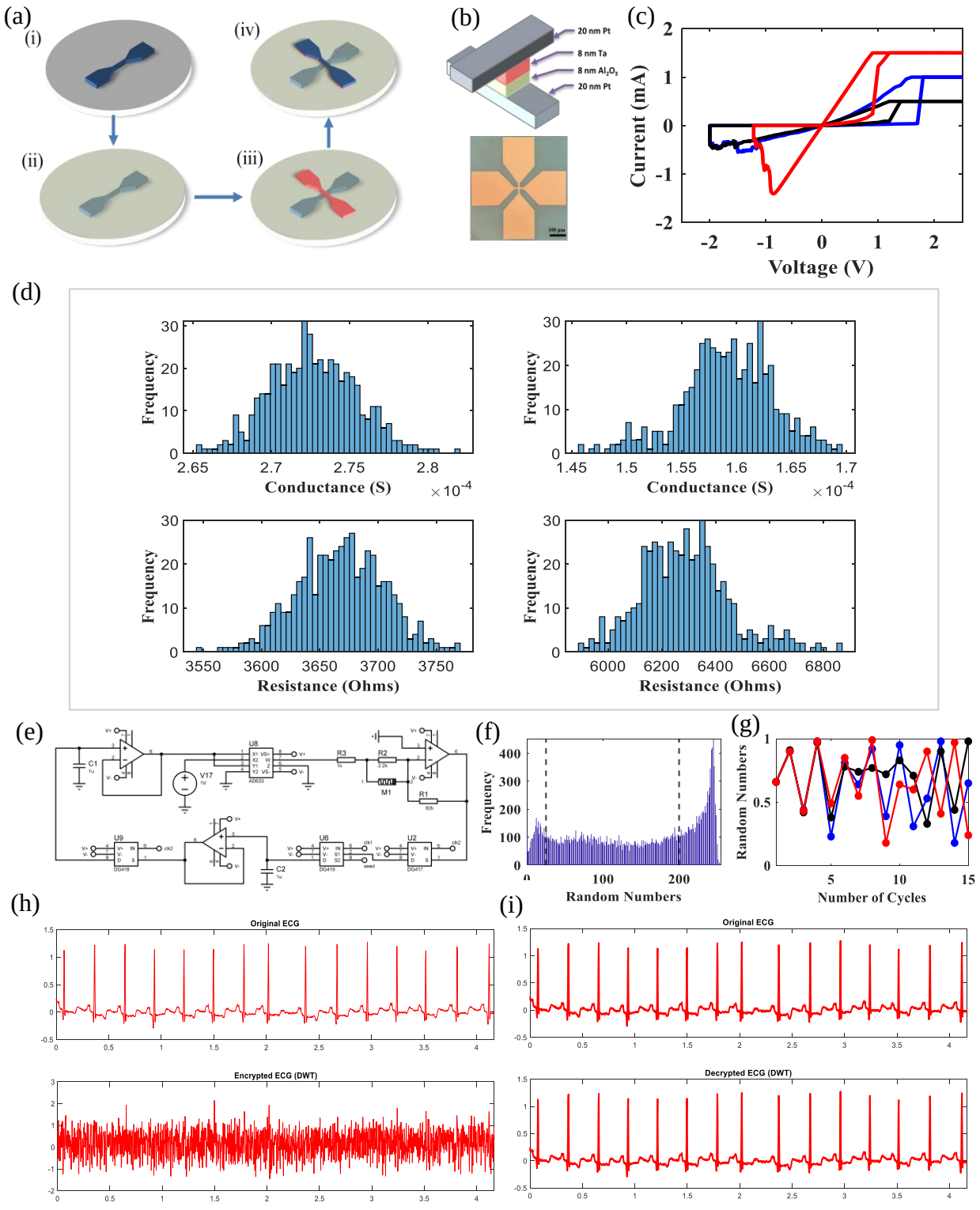

Fig. 1: (a) fabrication process of memristor, (b) memristor structure and optical image, (c) I-V characteristics, (d) histogram of conductance and resistance fluctuation (e) memristor enhanced logistic map based RNG circuit, (f) histogram of random numbers, (g) 3 RNG sequences started with same seed, (h) ECG signal encryption and (i) decryption using the RNG sequences.