Hardware Demonstration: Return Map Immune Lorenz Based Chaotic Stream Cipher in Circuitry

Daniel Brown, Ava Hedayatipour, Md Majumder, Garrett Rose, Nicole McFarlane, Donatello Materassi
School of Electrical Engineering and Computer Sience
University of Tennessee
Knoxville, TN 37996
Email: ahedaya1@vols.utk.edu

***Abstract*—Two similar chaotic systems, when appropriately coupled, can synchronize their states. This fundamental phenomenon has paved the way to the use of chaos as a means to encrypt messages. Indeed, a transmitter can produce a chaotic signal to mask a plain message and a synchronized receiver can invert this procedure to recover the original message. The most simple implementations of this encryption technique are, however, vulnerable to return map attacks. Using a time-scaling factor to further obfuscate the modulation process, we provably gain immunity against a return map. This live demonstration showcases return map immune chaotic stream cipher in circuitry based on a Lorenz system.**

I. DESCRIPTION OF THE RESEARCH

Chaotic encryption aims at providing security through masking a plain text with a chaotic signal originated by a chaotic system that is highly sensitive to system parameters and initial conditions [1], [2]. Methods exist to use both discrete maps [3] and continuous system models [4]. This demonstration makes use of a scheme based on a continuous system. Specifically, it uses a Lorentz system model to mask a binary plain text message using a technique known as Chaotic Shift Keying (CSK). The main advantage of continuous methods is the use of a minimal amount of processing power to obtain the cipher text. The power consumption can be several orders of magnitude lower than the power consumption required by a microprocessor to implement a standard digital encryption technique. The demonstration setup consists of the transmitter circuits, receiver circuit, a decision making block, and laptop with custom control and interfacing software for display.

II. VISITOR EXPERINECE

In our study the base Lorenz system has the form:

$$\dot{x} = k\sigma(x - y) \tag{1}$$

$$\dot{y} = k((\beta - z)x - y) \tag{2}$$

$$\dot{z} = k(xy - \rho z) \tag{3}$$

These equations are implemented in CSK system described by the block diagrams in Figure 1 and Figure 2. Figure 1 represents the encryption transmitter design and the receiver system is shown in Figure 2. The Gaussian noise is added into the transmitted state x_1.

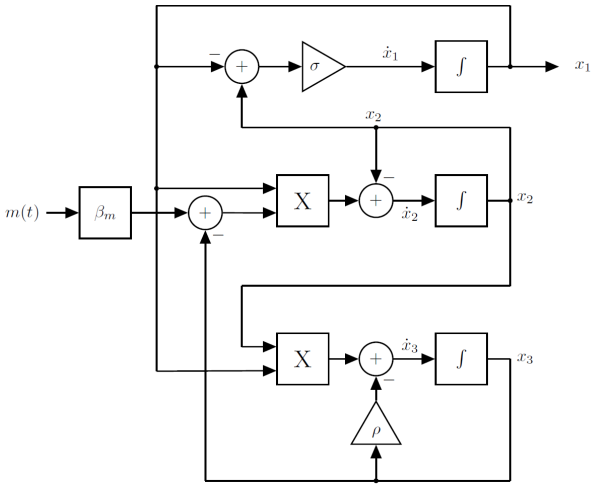


Fig. 1. Block diagram of the transmitter for the CSK system.

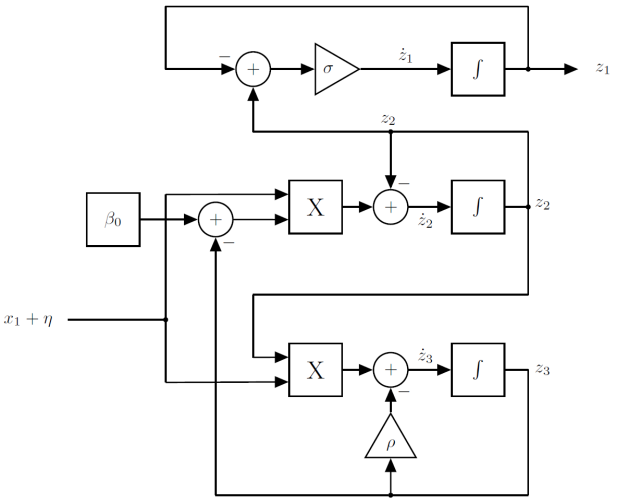
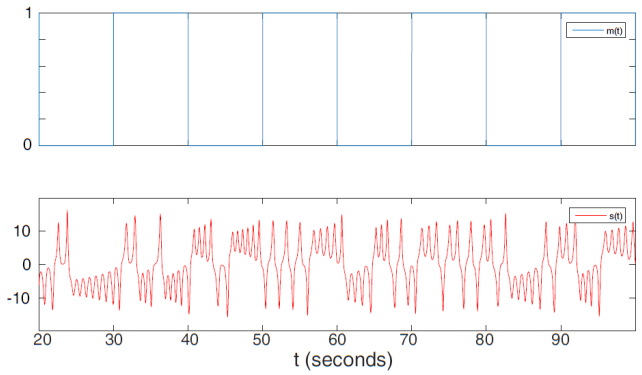
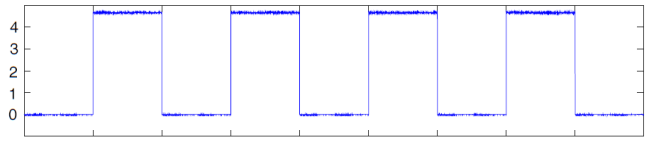


Fig. 2. Block diagram of the receiver for the CSK system.

However standard CSK schemes have been proven insecure against return map (RM) attacks. The return map attack monitors the transmitted state's local minima and maxima to detect transition from 0 bits to 1 bits and viceversa. More secure implementations of CSK can defeat RM attacks by introducing a a time-scaling factor in the chaotic modulation. However, the time-scaling factor needs to satisfy certain properties in order



(a)



(b)

Fig. 3. a)The sent signal x1(t) vs the message m(t). b) Real world data gathered.

to be also secure against return-time map (RTM) attacks.

To make a system secure to these attacks, we realize a Lorenz based chaotic system with an appropriate time-scaling factor, creating a Time Scaling Chaotic Shift Keying (TS-CSK) encryption system. The decoding is achieved by using a periodic averaging in cascade with a thresholding decision block. The threshold level is an important parameter that need to be carefully selected in order to guarantee a reliable decryption of the transmitted bits. This value is optimized experimentally. Once a decision is made for each potential bit, this information is then tested against m(t).

In our demo Data is then gathered as a single ended input. One channel collecting $\Phi 1(t)$, a synchronization test output determined as $x_1 - z_1$. The second channel is used to gather the message being sent from the NANO device. Figure 3 shows the response of the transmitted signal x1(t) in relation to the encrypted message m(t), Figure 3a, and the real world data gathered, Figure 3b.

To implement the chaotic encryption in circuitry, we use operational amplifiers and specialized semiconductor integrated circuits. The message is an alternating bit pattern that, most likely, is the most challenging signal to decode for the receiver. The message is also tuned in frequency to provide a reasonable data transfer rate and to take into account limitations in available data acquisition equipment. This PCB designed TS-CSK system and decision engine is depicted in Figure 4 and Figure 5.

To have our setup we couple the transmitter and receiver. A 480W ATX computer power supply provides both the 5V and differential $\pm$12V. Digital output of an Arduino NANO creates message m(t). The NANO would receive characters from a MATLAB script through the serial UART port. The frequency, bit padding, character and start send command is received

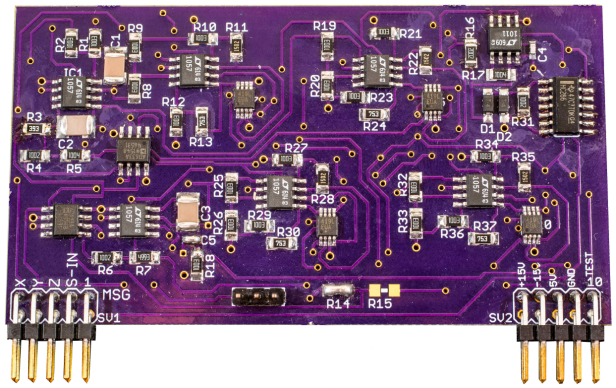


Fig. 4. Constructed TS-CSK system PCB.

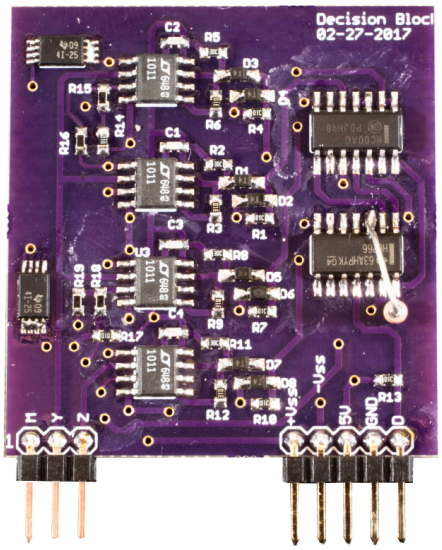


Fig. 5. Constructed Decision Engine PCB.

through the UART port . The NANO can send one character (8 bits) at a time. A second pin from the NANO is used as a falling-edge trigger to synchronize the data acquisition (DAQ) device with the character being sent. Data acquisition is accomplished using a National Instruments USB-6008 DAQ device. The device is capable of being triggered externally, has eight 12-bit single ended or differential analog inputs, and has a single channel max sample rate of 10,000 samples per second.

In our demo we show that any ASCII character can be encrypted, sent with the transmitter and then received. The characters would be sent with Matlab and received with a data acquisition.

REFERENCES

[1] L. M. Pecora, and T. L. Carroll, "*Synchronization in chaotic systems*," Physical review letters, vol. 64, no. 8, pp. 821, 1990.

[2] J. Lu, X. Wu, and J. Lu, "*Synchronization of a united chaotic system and the application in secure communication*," Physics Letters A, vol. 305, no. 6, pp.365 370, 2002.

[3] G. Makris, and I. Antoniou, "*Cryptography with chaos*," 5th Chaotic modelling and simulation international conference, pp. 12 - 15, 2012.

[4] J. M. Liu, and S. L. Tsimring, "*Digital communications using chaos and nonlinear dynamics*," Springer Science and Business Media, 2006.