Secure Communication via Chaotic Cryptography

Emiliia Gelóczi*, Nico Mexis*, Nikolaos Athanasios Anagnostopoulos*†, Florian Frank*, Tolga Arul*†, Stavros G. Stavrinides‡, and Stefan Katzenbeisser*

*Faculty of Computer Science and Mathematics, University of Passau, Germany
†Computer Science Department, Technical University of Darmstadt, Germany
‡School of Science and Technology, International Hellenic University, Greece

34th Crypto Day, 9/10 June 2022

Various electronic devices, such as phones, computers, watches, etc., are more and more present in our everyday life. Electronics become more complex, interconnected, and smart; even a trivial light bulb, which until recently was serving only as a source of light, nowadays may constitute a smart device with several functions and a high level of customisation. Despite smart devices making our life more comfortable and seeming so attractive for usage, they pose a large threat to our personal data. They consume, use, and generate zettabytes of data that can be stolen and used by an adversary. Information leakage can happen during any operational phase; however, in our work, we discuss one of the most critical parts – communication between devices. In order to establish secure data transfer, there are already various approaches, most of which utilise cryptography.

Traditionally, chaos has been considered as something unordered and uncontrollable and, for this reason, the use of chaos in cryptography, a scientific field that has been dominated by strict mathematical algorithms, is not widespread. Nevertheless, a chaotic signal can produce a truly random set of numbers; this suits cryptographic purposes, e.g., in the area of stream encryption. In order to investigate the possibility of using chaos for secure communication, we propose a chaos-based cryptographic system. The overall architecture of the proposed system consists of a transmitter, a receiver, and a post-processing filter, as shown in Figure 1.

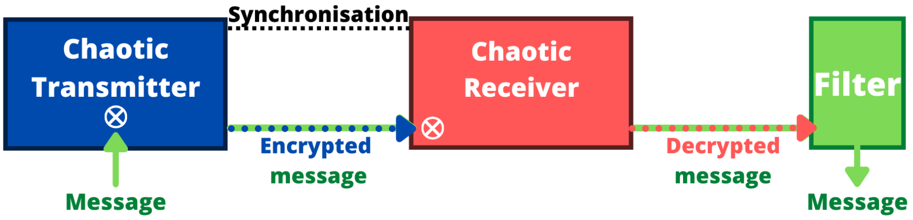

Figure 1: The overall architecture of the proposed system.

Experimental results using a variation of the Chua circuit presented by Kennedy (1992) confirm the good quality of communication and encryption

crypto day matters 34 (2022)
Beiträge vom 34. Kryptotag, 09.-10. Juni 2022, online.
doi:10.18420/cdm-2022-34-01

between the transmitter and the receiver. These results have been further validated by relevant simulations utilising either the aforementioned Chua circuits, or Lorenz-like chaotic circuits introduced by Li, Chu, Zhang & Chang (2009).

Internally, the transmitter and the receiver have similar architectures. Both of them utilise the same chaotic circuits in order to produce analogue chaotic signals. After digitising the analogue chaotic signal, using the technique described by Stavrinides, Anagnostopoulos, Miliou, Valaristos, Magafas, Kosmatopoulos & Papaioannou (2009), a random binary stream is generated. As the transmitter and the receiver are synchronised, we get the same stream of random numbers, which allows the binary message signal to be reliably encrypted and decrypted using the XOR operation. As a result of the system's operation, a signal identical to the initial message can be obtained at the receiver. Potential glitches and other noise are eliminated by using an RC low-pass filter. Relevant time series of the initial message, the encrypted signal, and the decrypted message, obtained using the Chua chaotic circuits, are shown in Figure 2.

An advantage of the described chaos-based secure communication system is that the probability of guessing the original message is less than 50%, as the attacker needs to correctly predict not only the period of the message being transmitted but also the correct value of each of the message bits.

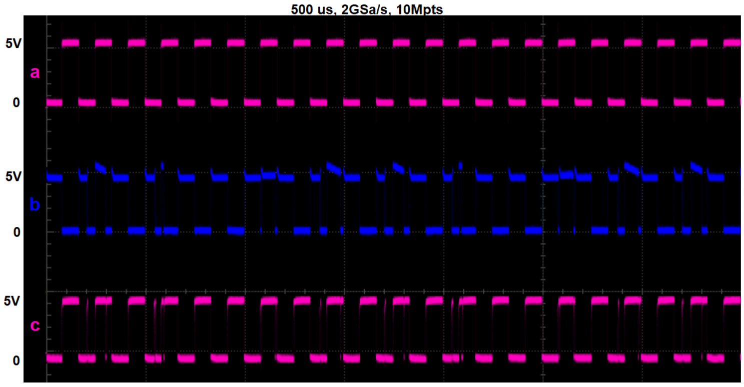

Figure 2: a) The initial message, b) the encrypted signal, and c) the decrypted message, for the secure communication system implemented using Chua circuits.

References

Michael Peter Kennedy (1992). Robust OP Amp Realization of Chua's Circuit. *Frequenz* **46**(3-4), 66–80. URL `https://www.degruyter.com/document/doi/10.1515/FREQ.1992.46.3-4.66/html`.

Xian-Feng Li, Yan-Dong Chu, Jian-Gang Zhang & Ying-Xiang Chang (2009). Nonlinear dynamics and circuit implementation for a new Lorenz-like attractor. *Chaos, Solitons & Fractals* **41**(5), 2360–2370. ISSN 0960-0779. URL `https://www.sciencedirect.com/science/article/pii/S0960077908004219`.

Stavros Stavrinides, Antonios N. Anagnostopoulos, Amalia N. Miliou, Antonios Valaristos, Lykourgos Magafas, Konstantinos Kosmatopoulos & Stavros Papaioannou (2009). Digital Chaotic Synchronized Communication System. *Journal of Engineering Science and Technology Review* **2**. URL `http://jestr.org/downloads/volume2/fulltext1609`.