Chapter 16
Control–Theoretical Concepts in the Design of Symmetric Cryptosystems

Gilles Millérioux
University Henri Poincaré of Nancy, France & Research Center on Automatic Control of Nancy (CRAN), France

José María Amigó
University Miguel Hernandez of Elche (UMH), Spain & Centro de Investigación Operativa, Spain

ABSTRACT

In this chapter, it is shown how control-theoretical concepts can be useful in the design of symmetric cryptosystems. The authors first provide some background on cryptography with special emphasis on symmetric ciphering and, more specifically, on stream ciphers. It is explained how some permutation or substitution primitives can be derived from chaotic dynamical systems for cryptographic purposes. After a review of the most popular synchronization-based cryptosystems, a comparative study between these chaotic cryptosystems and the conventional symmetric ciphers, specifically stream ciphers, is carried out. In particular, it is shown that message-embedded chaotic ciphers and conventional self-synchronizing stream ciphers are structurally equivalent under the so-called flatness condition, a condition borrowed from control theory.

1 INTRODUCTION

The considerable progress in communication technology during the last decades has led to an increasing need for security in information exchanges. In this context, cryptography plays a major role as information is mostly conveyed through public networks. The main objective of cryptography is, precisely, to conceal the content of messages transmitted through insecure channels, to unauthorized users or, in other words, to guarantee privacy and confidentiality in the communications. Since the early 1960s, cryptography has no longer been restricted to military or governmental concerns, what has spurred an unprecedented development of it. At the same time, this development benefited very much from the ad-
Advances in digital communication technology in form of new and efficient ways of designing encryption schemes. Despite the diversity of cryptographic techniques, two major classes are typically distinguished: public-key ciphers and symmetric-key ciphers (also called private-key ciphers).

Let us shortly recall that modern cryptography originates in the works of Claude Shannon after World War II (Shannon, 1949). Shannon’s ideas substantiated in form of substitution-permutation networks, that are at the heart of the Lucifer encryption algorithm, designed by IBM in the late 1960s and early 1970s (Pieprzyk et al, 2003). One of the key dates in the recent history of cryptography is 1977, when the symmetric cipher Data Encryption Standard (DES) was adopted by the U.S. National Bureau of Standards (now the National Institute of Standards and Technology ---NIST), for encrypting unclassified information. DES is now in the process of being replaced by the Advanced Encryption Standard (AES), a new standard adopted by NIST in 2001. Another milestone is 1978, marked by the publication of RSA, the first full-fledged public-key algorithm. This discovery not only solved the key-exchange problem of symmetric cryptography but, most importantly, did it open new whole areas (like authentication and electronic signature) in modern cryptology. Among symmetric-key ciphers, stream ciphers are of special interest for high speed encryption, like in satellite communications, private TV channels broadcasting, and networked embedded systems. They are mainly based on generators of complex sequences, which must be synchronized at the transmitter and receiver sides. Stream ciphers have received much attention recently. Two European projects have influenced this evolution: The project NESSIE within the Information Society Technologies (IST) Programme of the European Commission, which started in 2000 and ended in 2004, followed by ECRIPT1, launched on February 1st, 2004. Sponsored by ECRIPT, ESTREAM is a multi-year effort to identify promising software- and hardware-oriented algorithms with the aid of proposals from industry and academia.

Chaotic behavior is one of the most complex dynamics a nonlinear system can exhibit. One of the formal definitions of chaos is due to R.L. Devaney (Devaney, 1989). A dynamical system is said to be chaotic in the sense of Devaney if it fulfills two properties: Transitivity and density of periodic points. It can be shown that sensitivity to the initial condition, which is the property mostly associated with chaotic behavior, is actually a consequence of those two other properties. Roughly speaking, a system is said to be sensitive to initial conditions if a small change in the initial condition drastically changes the behavior of a system in the long run, thus making long-term predictions unfeasible in practice. Complex dynamics had its beginnings in the work of the French mathematician Henri Poincaré (1854-1912), who also recognized the practical unpredictability of such systems. Sensitive dependent phenomena were highlighted by Edward Lorenz in 1963 while simulating a simplified model of convection. But it was the paper “Period Three Implies Chaos” by Li and Yorke in 1975 (Li, & Yorke, 1975), where the word “chaos” was coined in the framework of dynamical systems, which triggered a tremendous interest in this kind of phenomena. Since then a great number of applications have been proposed in such disparate areas as mechanics, physics, biology, economy, engineering, avionics or weather forecasting.

Signals generated by chaotic systems are broadband, noiselike and present random-like statistical properties, in spite of being deterministic. This makes them a very convenient tool to implement the principles of confusion and diffusion required by Shannon for cryptosystems (Shannon, 1949; Massey, 1992). The first proposals in this direction were made around 1990 (Matthews, 1989; Habutsu et al, 1991). In 1990 entered the scene chaos synchronization (Carroll, & Pecora, 1991), a new technique for analog communication (Parlitz et al, 1993) whose potential for cryptography was soon exploited (Cuomo et al, 1993). Since then, many schemes have been proposed to mask information using the properties of chaos, either based on discrete chaotic maps or on the synchronization of signals. This new approach to
Related Content

A Model for Monitoring and Enforcing Online Auction Ethics
[www.igi-global.com/chapter/model-monitoring-enforcing-online-auction/23340?camid=4v1a](www.igi-global.com/chapter/model-monitoring-enforcing-online-auction/23340?camid=4v1a)

Data Reduction
[www.igi-global.com/chapter/data-reduction/29698?camid=4v1a](www.igi-global.com/chapter/data-reduction/29698?camid=4v1a)

Wild-Inspired Intrusion Detection System Framework for High Speed Networks (f|p) IDS Framework
[www.igi-global.com/article/wild-inspired-intrusion-detection-system/62315?camid=4v1a](www.igi-global.com/article/wild-inspired-intrusion-detection-system/62315?camid=4v1a)

Barriers Facing African American Women in Technology
[www.igi-global.com/chapter/barriers-facing-african-american-women/13451?camid=4v1a](www.igi-global.com/chapter/barriers-facing-african-american-women/13451?camid=4v1a)