19.5.
2. posudek

HTWK Leipzig - University of Applied Sciences
Faculty of Electrical Engineering and Information Technology
Prof. Dr.-Ing. Hendrik Richter

HTWK Leipzig

Review of the Dissertation Thesis
"Chaos-based Communication Systems"
by Volodymyr Lynnyk

submitted to the
Faculty of Electrical Engineering at the Czech Technical University in Prague

The dissertation thesis presented deals with design, analysis, test and application of chaos-based communication systems. These chaos-based communication systems rely upon and take advantage of synchronization, one of the most remarkable and interesting properties of chaotic systems.

Over the last few decades, theory and application of chaos have become an indispensable element in science and engineering. In the context of observing, analysing, constructing and controlling chaotic systems, synchronization - first reported by Pecora and Carroll in the beginning of the 1990s - is still one of the fields which is most actively researched. Although synchronization is mainly understood from a theoretical point of view, application of this property of chaotic dynamics, for instance to secure communication, is nevertheless still a main focus of interest. So, the topic of the thesis can be seen as being in the mainstream of current research in the field of nonlinear dynamics and chaos.

The main objective of the thesis is - based on an analysis of existing schemes and after discussing their shortcomings - to develop and test alternative methods for communication and encryption that explicitly use properties of chaotic systems. The author pursues this in the following way. After some introductory remarks, the first chapter reviews the theoretical and conceptual background for the work undertaken in the thesis. In it basic results in cryptography (definitions, classifications, and properties) are described. In addition, chaotic systems are introduced formally, and quantities for evaluating chaotic systems (Lyapunov exponent and Kolmogorov-Sinai-entropy) are given. The selection of these two quantities is not motivated, and only the Lyapunov exponent plays a (minor) role in the further discourse. This is followed by an overview of communication schemes that use properties of chaotic systems, namely ergodicity and sensitive dependence on initial states and/or parameters. All main schemes (chaos shift keying, chaos-on-off-keying, differential chaos shift keying, frequency-modulated chaos shift keying etc.) are briefly described. The main application of these schemes is private communication. So, the link to cryptographic systems is made by discussing chaos-based cryptosystems, their advantages and disadvantages as well as possible strategies for attacking them.

These chapters mainly setting the background for the thesis work are followed by a first main contribution of the dissertation, the employment of Generalized Lorenz systems (GLS) in chaos-based communication. GLS have been introduced by Čelikovský & Chen and can be

seen as a general class of 3D nonlinear continuous-time systems capable of chaotic solutions. The well-known Lorenz system which was the first model numerically showing chaos as early as 1963 appears as a special case of the GLS. The GLS enjoy some nice mathematical properties. In particular, it can be proved that it is observable (and hence synchronizable) with an exponentially decaying error dynamics. These properties and their significance for chaotic cryptosystems are discussed in the beginning of Chapter 3. Based on these results a first contribution of the thesis is to show by mathematical proof how these properties modify for parameter mismatch. The proof is based on a Lyapunov function approach frequently used in control theory and yields the necessary stability conditions that can be interpreted in terms of synchronizability. Some interpretation and algebraic manipulation further give upper and lower bounds for the error dynamics scaling to the parameter mismatch and its time characteristics.

Next to these results, a description of the Anti-synchronization Chaos Shift Keying (ACSK) is given, whose development, study and security analysis is a second major contribution of the thesis. The ACSK modifies and improves classical chaos shift keying methods with separating the key and the message. Hence, for the receiver there is no need to achieve synchronization by using the message signal alone. This improves upon classical chaos key shifting as it allows to increase the speed of the data transmission considerably. The ACSK is implemented using the GLS studied earlier. A brief numerical study appears to confirm the theoretical results regarding the GLS.

A third main contribution of the thesis is an analysis of synchronization properties of the GLS using the theoretical framework of dynamical complex networks, which uses elements from random graph theory. Using this framework, synchronizability of a given number of GLS is considered. Again, using a Lyapunov function approach theoretical results regarding unidirectional and bidirectional synchronization are derived for two-node networks. These results are briefly generalized for four-node networks using numerical experiments. The thesis concludes with a summary of the findings, and a pointer at future research topics.

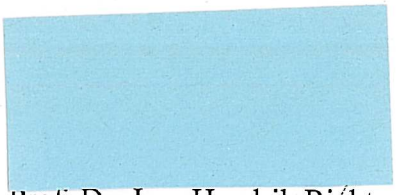
To summarize, the considered topics and contributions given in the thesis are in agreement with the main objectives set out above. This applies to the content as well as to the methodology used. In line with modern approaches to tackle problems in system dynamics and control, the methods used fall into two categories: (i.) formal mathematical treatment and description characterized by a theorem-preposition-proof-remark-structure and (ii.) applying an experimental approach using numerical simulation. Both methodological strains are used in the thesis in an appropriate manner. The formal mathematical treatment is sufficiently strict and detailed, and uses commonly known mathematical techniques. The numerical experiments are logically designed, performed and reported. However, I feel that they could be slightly more elaborated. For instance, the relationship between parameter mismatch and error dynamics that has been derived theoretically is briefly studied using numerical results in Chapter 3.4, but no dependency on different initial conditions is given. The same applies for the numerical investigation of four-node networks, which is rather a bit sketchy. Further, as numerical

conditions are crucial, it would have been interesting to have at least a short discussion on the influence of different solver types and their parameters.

The content of the thesis, in particular the usage of GLS within the ACSK framework, is of value to the research community devoted to applying chaotic systems for communication purposes. As the ACSK is a real improvement over classical CSK methods, there is the hope that this might open the door to real-world applications of the scheme.

Remarkable is that the candidate has (collaboratively) written nine papers related to the topics of his dissertation which are published in peer reviewed international conference proceedings and journals. The amount and the quality of these published works are above international academic standards for Ph.D students, which together with the thesis show the creativity of the presented scientific work. It should also be positively noted that the author has written his thesis in English, hence making the content and the results easily accessible to the international research community. In view of this, the small amount of mistakes in English grammar and style should not be overrated. However, prior to a (possible) publication of the thesis they should be corrected.

The author of the thesis proved to have an ability to perform research and to achieve scientific results. I do recommend the thesis for presentation with the aim of receiving the Degree of Ph.D.



Prof. Dr.-Ing. Hendrik Richter, Leipzig, 16 May 2010