INFORMATION OF THE DOCTORAL THESIS

Thesis title: *"On a pseudo-random number generation algorithm based on interleaved nonlinear sequence generation method with a large order"*

Specialization: Electronic Engineering

Code: 9.52.02.03

PhD. Candidate: DANG VAN TRUONG

Scientific supervisors:

Prof. D.Sc NGUYEN XUAN QUYNH

Training institution: Posts and Telecommunications Institute of Technology

ACADEMIC CONTRIBUTIONS OF THE THESIS

Pseudo-random sequences based on m-sequences are a problem that has always been interesting in recent times, as these sequences have had many applications in electronics-telecommunication and information security. The thesis has studied architecture, characteristics, and properties of the interleaved nonlinear sequence as well as the requirements in its application in information security. Since then, a solution for using an interleaved nonlinear sequence has been proposed to ensure the security requirements but still can be implemented in practice. The new contributions of the research process shown in the thesis are as follows:

(1) Propose a solution for interleaved nonlinear sequence generation based on step decomposition technique and partial calculation of interleaved orders set. We can apply this solution in practical implementation to generate an arbitrary-sized segment of this sequence.

(2) Propose an effective algorithm to generate interleaved nonlinear sequence with a large order, analyze and evaluate the proposed algorithm in terms of computational complexity, storage complexity, and experimental results. The algorithm has computational complexity asymptotically to $O(n^3)$, where n is the degree of the m-sequence. By exploiting a feature of the interleaved sequence parameter, this algorithm has an advantage over the conventional squaring and multiplying algorithm.

APPLICATIONS, PRACTICAL APPLICABILITY AND FUTURE WORKS

From the proposes given in the thesis, we have a feasible plan to apply interleaved nonlinear sequences in information security in practice with a high-security level without using too much processing power and computational resources. In addition to the application of these sequences in cryptographic engineering, many engineering fields can apply interleaved nonlinear sequences as pseudo-random sequence generators with different purposes.

Future works

Proposing a new cryptographic algorithm requires careful consideration of the security of the algorithm in many aspects before putting the cryptosystem into practical use. We also need further studies on crypto analysis for interleaved and nonlinear interleaved sequences.

Another work that needs further research is the solution to efficiently implement interleaved sequences on $GF(p^n)$ with large prime p ($p>2$) in both environments: computer software and hardware processing devices. We also need to study the efficient use of the output sequence on $GF(p^n)$, for example as a method to convert the sequence from q-ary to binary.

Scientific supervisor	**PhD. Candidate**
Prof. D.Sc Nguyen Xuan Quynh	**Dang Van Truong**