# Random Number Generator Based on Biometric Approach. Testing the Cryptographic Strength

Ekaterina Andreeva, Konstantin Zhidanov
Saint-Petersburg State University of Aerospace Instrumentation
Saint-Petersburg, Russia
{eandreeva89, konstantin.zhidanov}@gmail.com

**Abstract**

Security of medical information is the current problem in the modern society. Every year appear more and more telemedicine systems and m-health applications, for diagnosis of human condition and maintenance of life-support. Growing technological complexity of electronic medical devices leads not only to increased efficiency, but also increase risk of loss of personal information. The most important problems of information security in healthcare are access control to medical personal data and security data transmission. These problems are especially important in systems of monitoring human condition, used sensors. Due to constraints of energy, memory and computation power secure communication between sensors is not a trivial problem. The biometric technology using heart sounds and acoustic characteristics of the circulatory system allows constructing flexible information security systems, adapted to the specific characteristics of medical devices. This approach gives ability to use data which medical device gets during human condition monitoring. This feature allows not complicating medical device by information security system. Acoustic characteristics of the circulatory system allow generating a common key for the symmetric cryptosystems. Such acoustic characteristics of the circulatory as human heart sounds and inter-pulse interval are using in order to receive groups of similar random numbers to encrypt and decrypt the symmetric key.

In this article, ability of using inter-pulse interval for generating random values to develop a common encryption key is analyzed. To assess the effectiveness of using inter-pulses intervals as a source of random common key for symmetric cryptosystems have been analyzed the properties of heart rate variability. Analysis of heart rate variability will help answer the question: “Is there a correspondence between values of inter-pulse intervals and cryptographic random number generator.” Values of inter-pulse intervals are obtained as a result of a physical process, i.e. as a result of human heart work. As it is known, random number generators, working on the basis of the physical process can generate truly random numbers. To confirm the hypotheses were used methods, which are commonly used in medical practice for heart rate variability analysis - time domain methods, geometric methods, integral HRV (include autocorrelation analysis).