11th International Conference - IcETRAN 2024
Niš, Serbia, June 3-6, 2024

Artificial Intelligence Section (VII)
INVITED PAPER:

"Perfectly secret system for voice transmission based on common randomness"

Jelica Radomirović, Sara Čubrilović, Zvezdana Kuzmanović, Zoran Banjac, and Milan Milosavljević
Institute VLATACOM
Belgrade, Serbia

Abstract: This paper presents a system for secure digital voice signal transmission over the GSM mobile network. The cryptographic part of the system is based on Vernam's code, which requires the same speed of generating secret symmetric keys as the basic information flow in the main channel. The system for generating and distributing secret keys for Vernam's system is realized based on the correlation properties of the locally synthesized speech signal of the transmitter and the corresponding receiving speech signal. By applying the method of sequential distillation of secret keys (SKD) on the mentioned source of common randomness, the generation speed of up to 28 kb/s is ensured, which is more than enough to maintain the absolute secrecy of Vernam's cipher. The price that needs to be paid is the necessity of having an additional authenticated public channel through which the SKD protocol is performed. The privacy amplification block, as a necessary part of the SKD protocol, was implemented using machine learning methods, to reliably estimate the conditional Renyi entropy of the second order. According to our knowledge, this is the first autonomous, perfectly secret system for voice transmission over the GSM network without explicit prior generation and distribution of secret keys.

Short biography:

Jelica Radomirović was born on July 3, 1997. in Belgrade. She graduated from the Mathematical Grammar School in Belgrade, after which she entered the Faculty of Electrical Engineering in 2016. She was a student at the Department of Signals and Systems and graduated in 2020 with an average grade of 9.13. She completed her master's studies at the Faculty of Electrical Engineering in Belgrade, on the signals and systems module, in 2021 with an average grade of 9.83. She is currently a PhD student at the Faculty of Electrical Engineering, studying the module of Systems control and signal processing. Since 2021, she has been employed at the Vlatacom Institute of High Technologies as an R&D engineer, where she deals with the application of machine learning in cryptography systems. In addition, the areas of work are systems of absolute secrecy, artificial intelligence, machine learning, signal, and data processing. She is the author and co-author of several scientific papers in international journals.