A5-Based GSM Cryptosystem Implementation and Analysis

Dr. Daniel Okunbor

Professor of Computer Science
Department of Mathematics and Computer Science
Fayetteville State University, Fayetteville, North Carolina 28301 USA
diokunbor@uncfsu.edu

In this research, we would explore cryptosystems implemented in the Global System for Mobile (GSM) Communications. GSM is a standard developed by the European Telecommunications Standards Institute (ETSI) to describe the protocols for second-generation (2G) digital cellular networks used by mobile phones. It was first deployed in Finland in July 1991. It is recently considered the de facto global standard for mobile communications – with over 90% market share, operating in over 219 countries and territories. A commonly used cryptosystem for GSM communications is the A5 ciphering algorithm. There are seven of such ciphers, designated as A5/1, A5/2, ..., A5/7. These are stream ciphers based on a combination of Linear Feedback Shift Registers (LFSRs) with irregular clocking and non-linear combiner. The A5/1 uses 3 LFSRs and A5/2 uses 4 LFSRs. In this research, we will develop a general-purpose software Python library for A5 implementation. We would also consider the parallel implementation of A5 using Graphics Processing Unit (GPU) clusters. The simplicity and the linear arrangements of the flip-flop based shift registers and the internal state independency make the algorithms suitable for distributed computing.