ABSTRACT

Security system in GSM network (Global System for Mobile Communication) is necessarily needed to avoid the information robbing by the others side or groups who are not responsible. Security system in GSM network is implemented in A5 algorithm of cryptography method, which is a voice coding method in real time communication, goes on between MS (Mobile Station) and BS (Base Station).

A5/1 method is a fervent version of A5 Algorithm in GSM networks that symmetric cryptography algorithm with stream chiper encryption technique which consists of 3 LFSR (Linier Feedback Shift Register) in 19, 22 and 23 degree. LFSR is a linier back forward shift register as a line of random numbers. While TMS320VC33 is DSP (Digital Signal Processor's) Card which has operation velocity reaches 75 MIPS (Million Instruction Operations per Second) or 13.34 ns per instruction, there are probabilities for doing digital signal processing in real time. This final task specially discusses about planning and implementing of A5/1 algorithm cryptography uses TMS320VC33 DSP Card where the parameters have analyzed, such as time processing, avalanche effect, brute forced attack and variance.

From the tested results have made a conclusion that system can be realized with processing time is 2.607516 ms which calculated based on duty cycle. Value of avalanche effect based on changing of 1 key bit reaches 45.39473%, while based on changing of 1 plaintext bit or ciphertext only 0.893%. Variance value is 6.0982, while time to brute forced attack is $1.406791788 \times 10^{28}$ year.

Key words: A5/1 Algorithm, DSP Card TMS320VC33, GSM (Global System for Mobile Communication), Time Processing, Avalanche Effect, Variance, Brute Forced Attack