|  |  |
| --- | --- |
| **LABORATORIUM BEZPIECZEŃSTWA SYSTEMÓW TELEINFORMATYCZNYCH** (CZ. 1) | |
| **Wykonali:**  Jan Kowalski, Adam Nowak | Data oddania  15.04.2020 r. |
| **Podstawa opracowania:**  J. Smith, A. Newman, „Audio random number generator and its application”, International Journal of Computer Science, vol. 34, pp. 123-129, 2019. | |
| **Systematyczny przegląd literatury:**   1. baza danych IEEE Xplore, 2. słowa kluczowe: TRNG, PC, Audio, 3. okres publikacji: 2015-2019, 4. … 5. zdefiniowany pseudokod algorytmu; 6. spełniane testy NIST. | |
| **Analiza źródła entropii:**  Algorytm wykorzystuje mikrofon komputerowy do nagrywania i digitalizacji dźwięku otoczenia za pomocą interfejsu API Waveform Audio Interface (WAV). W pracy wykorzystano częstotliwość próbkowania 44,1 kHz, rejestrując 44100 próbek na sekundę zapisywanych jako zmienne 8-bitowe. Źródło szumu ograniczono do trzech najmniej znaczących bitów każdej próbki (LSB) zidentyfikowanych jako wykazujące wzorce losowe.    Entropia wyliczona zgodnie ze wzorem: , dla powyższego rozkładu wynosi **6,761** bita.  Wyniki testu statystycznego NIST 800-22 | |
| **Metoda poprawy właściwości statystycznych:**  Aby przetworzyć pobrany szum audio, każde pobrane 256 bitów jest mapowane na osiem różnych liczb zmiennoprzecinkowych z 32-bitową precyzją, które są używane jako początkowe stany ośmiu miejsc sieci. Następnie pseudolosowy generator kratowy ze sprzężonym mapowaniem (CML-MPRBG) realizujący zmianę stanu zgodnie z mapą logistyczną:  dla *N* iteracji i wyodrębnia *k*-bit bitów z ostatnich 32 stanów chaotycznych w ośmiu miejscach sieci w celu utworzenia 256-bitowej liczby losowej. W przyjętej implementacji mapą logistyczną jest lokalna mapa chaotyczna , natomiast , i .    Entropia wyliczona zgodnie ze wzorem: , dla powyższego rozkładu wynosi **7,9998** bita.  Wyniki testu statystycznego NIST 800-22 | |
| **Metoda poprawy właściwości statystycznych przez zastosowanie AES-256 CTR (gr Kubczak) / SHA3-256 (gr Nikonowicz):**  Aby przetworzyć pobrany szum audio, każde pobrane 128/256 bitów jest poddawane działaniu **AES-256 CTR/ SHA3-256**    Entropia wyliczona zgodnie ze wzorem: , dla powyższego rozkładu wynosi **7,9999** bita.  Wyniki testu statystycznego NIST 800-22 | |
| **Uwagi:** | |