ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1998
Seria: INFORMATYKA z. 34 Nr kol. 1381

Antoni NIEDERLIŃSKI, Jarosław FIGWER
Politechnika Śląska, Instytut Automatyki

SZYFROWANIE DANYCH Z WYKORZYSTANIEM WIELOSINUSOIDALNYCH SYGNAŁÓW LOSOWYCH

Streszczenie. W pracy przedstawiono podstawy teoretyczne metody szyfrowania danych z wykorzystaniem wielosinusoidalnych sygnałów losowych. Ideą proponowanej metody jest wykorzystanie kolejnych znaków tekstu do generowania losowych faz sygnałów wielosinusoidalnych. Wygenerowane fazy oraz wybrane amplitudy poszczególnych składowych sinusoidalnych pozwalają na skonstruowanie widma sygnału wielosinusoidalnego, które jest transformowane do dziedziny czasu za pomocą algorytmu szybkiego przekształcenia Fouriera dając w wyniku zaszyfrowany tekst w postaci realizacji wielosinusoidalnego sygnału losowego. Metoda jest zilustrowana przykładem.

DATA ENCRYPTION USING MULTISINE RANDOM TIME SERIES

Summary. The paper presents theorethical foundations of an encryption method based on multisine random time-series. Its main idea is to use consecutive characters of the plaintext to generate random phase shifts for all sine components of the multisine random time-series. These random phase shifts together with chosen amplitudes are used to construct the discrete Fourier transform of the corresponding multisine random time-series. The obtained spectrum is transformed into the time domain by using any fast Fourier transform algorithm resulting in the encrypted plaintext of the form of a multisine random time series. The method is illustrated by an example.

1. Wstęp

W ostatnich dwóch dziesięcioleciach nastąpiła eksplozja jawnych badań naukowych w dziedzinie kryptografii. Opublikowane wyniki pozwalają na stosowanie technik kryptograficznych do ochrony danych wykorzystywanych w codziennym życiu. Ochrona ta ma

szczególne znaczenie przy przechowywaniu i przesyłaniu poufnych informacji za pomocą powszechnie dostępnych sieci komputerowych. W wielu stosowanych do tego celu popularnych metodach szyfrowania wykorzystuje się techniki generowania pseudolosowego białego szumu ([3], [4], [11], [16]) po to, by usunąć z danych podlegających szyfrowaniu korelacje pomiędzy jego kolejnymi elementami. Przedstawiona poniżej nowa idea szyfrowania nawiązuje do tych metod. Nie jest ona jednak wynikiem badań kryptograficznych, lecz produktem ubocznym badań nad doświadczalną identyfikacją modeli matematycznych z zastosowaniem wielosinusoidalnych sygnałów pobudzających, por. [6], [9], [13]. Badania te, dosyć nieoczekiwanie dla autorów, stworzyły możliwość sformułowania nowego rozwiązania problemu syntezy dowolnych sygnałów losowych o zadanych właściwościach widmowych (por. [5], [7], [8], [14]). Rozwiązanie to otwiera również drogę do nowej techniki szyfrowania, której istotą jest *zanurzenie* szyfrowanego tekstu w widmie fazowym sygnału będącego realizacją procesu losowego o dowolnych, zadanych właściwościach widmowych. W szczególnym przypadku proces ten może być białym szumem.

Punktem wyjścia metody jest definiowanie realizacji wymienionego procesu losowego w dziedzinie częstotliwości za pomocą periodogramu wielosinusoidalnego sygnału losowego. Aby ten sygnał syntezować, należy dla jego periodogramu wyznaczyć widma amplitudowe i fazowe, a następnie poddać wypadkowe widmo zesplone odwrotnej transformacji Fouriera.

Przedstawienie periodogramu za pomocą widma amplitudowego i fazowego jest jednoznaczne w odniesieniu do widma amplitudowego i niejednoznaczne w odniesieniu do widma fazowego: ten sam periodogram można uzyskać dla jednego określonego widma amplitudowego i nieskończenie wielu różnych widm fazowych. Ową niejednoznaczność można wykorzystać do tego, by w widmie fazowym *zanurzyć* szyfrowane dane, np. w ten sposób, by kolejne wartości faz widma odpowiadały niezaszyfrowanym lub wstępnie zaszyfrowanym kolejnym znakom tekstu jawnego. W wyniku odwrotnej transformacji Fouriera widma zespolonego (z widmem amplitudowym determinującym periodogram i widmem fazowym zawierającym dane) otrzymuje się realizację procesu losowego, tzn. sygnał losowy o założonych właściwościach widmowych, będący zarazem nośnikiem danych, przy czym każdy znak tekstu jawnego jest reprezentowany przez wszystkie wartości tego sygnału. Odzyskanie tekstu jawnego jest możliwe na drodze poddania tego sygnału transformacji Fouriera, odtwarzającej pierwotne widma amplitudowe i fazowe. A więc zarówno na etapie szyfrowania, jak i deszyfrowania stosowane są algorytmy bardzo efektywne (szybka transformata Fouriera - FFT) i realizowane sprzętowo (procesory sygnałowe).

Należy podkreślić, że w szczególnym przypadku stosowania tej metody szyfrowany tekst może być *zanurzony* w sygnale, którego periodogram jest stały w całym zakresie

częstotliwości, a więc w białym szumie będącym sygnałem losowym absolutnie chaotycznym.

Podstawowym elementem przedstawionej idei jest wielosinusoidalny sygnał losowy, będący sumą harmonicznych składowych sinusoidalnych o deterministycznych amplitudach i losowych fazach. Sygnał taki jest szczególnie wygodnym *prototypem* dla syntezy procesów losowych o zadanej funkcji gęstości widmowej mocy [8], aproksymowanej periodogramem. W szczególnym przypadku można go użyć do syntezy skalarnych i wielowymiarowych ergodycznych białych szumów ([5], [7], [14]).

Organizacja artykułu jest następująca: (1) W punkcie pierwszym wprowadzono definicje wielosinusoidalnych sygnałów losowych i omówiono ich własności, ze szczególnym zwróceniem uwagi na wpływ losowych faz na stacjonarność i ergodyczność analizowanych sygnałów. (2) Zaproponowano metodę szyfrowania z wykorzystaniem algorytmu szybkiej transformacji Fouriera. Wprowadzono również dodatkowe zabezpieczenia, których celem jest zwiększenie odporności proponowanej metody na próby łamania. (3) Omówione teoretyczne podstawy metody szyfrowania zilustrowano poprzez przykład zaszyfrowania tekstu wiersza Lechonia „Poniedziałek" ([12]). W analizowanym przykładzie amplitudy poszczególnych składowych sinusoidalnych sygnału wielosinusoidalnego wybrano tak, by periodogram wielosinusoidalnego sygnału losowego był równy periodogramowi pewnej N-elementowej realizacji otrzymanej z generatora białego szumu o rozkładzie normalnym. Uzyskane tą drogą szyfrogramy zachowują się, z punktu widzenia statystyki, dokładnie tak, jak ciąg realizacji zmiennej losowej będącej białym szumem o rozkładzie normalnym.

2. Wielosinusoidalne sygnały losowe

N-elementowy (N parzyste) wielosinusoidalny sygnał losowy jest zdefiniowany w dziedzinie czasu jako suma $\frac{N}{2}+1$ harmonicznych sinusoid wraz ze składową stałą:

$$u^N(i) = \sum_{n=0}^{\frac{N}{2}} A_n \sin(\Omega n i + \phi_n), \tag{1}$$

gdzie:

- $\Omega = \frac{2\pi}{N}$ oznacza względną częstotliwość podstawową;
- Ωn $(n = 0, 1, \ldots, \frac{N}{2})$ oznacza kolejne harmoniczne względnej częstotliwości podstawowej w przedziale $[0, \pi]$;
- $i = 0, 1, \ldots, N-1$ oznacza kolejne chwile czasowe;

- A_n ($A_n \in \mathcal{R}$) oznacza amplitudę n-tej składowej sinusoidalnej;
- ϕ_n oznacza fazę n-tej składowej sinusoidalnej, przy czym faza ϕ_0 jest deterministyczna, a pozostałe fazy są losowe, niezależne oraz:
  - dla $n = \frac{N}{2}$ faza $\phi_{\frac{N}{2}}$ jest zmienna losową o rozkładzie Bernoulliego $\mathcal{B}\left(\frac{1}{2}, \{\alpha, \pi + \alpha\}\right)$:

$$P\left\{\phi_{\frac{N}{2}} = \alpha\right\} = P\left\{\phi_{\frac{N}{2}} = \pi + \alpha\right\} = \frac{1}{2}, \tag{2}$$

    gdzie $P\{X\}$ oznacza prawdopodobieństwo zdarzenia X,
  - dla $n = 1, 2, \ldots, \frac{N}{2} - 1$ fazy ϕ_n są zmiennymi losowymi o dowolnym rozkładzie gęstości prawdopodobieństwa określonym na pewnym zbiorze $\mathcal{S}(\phi_n) \subset [0, 2\pi)$.

Na podstawie definicji N-punktowej dyskretnej transformaty Fouriera wielosinusoidalny sygnał losowy można zapisać w dziedzinie częstotliwości ([5], [8]) jako:

$$U^N(j\Omega m) = \sum_{i=0}^{N-1} u^N(i) e^{-j\Omega m i} = \sum_{i=0}^{N-1} \sum_{n=0}^{\frac{N}{2}} A_n \sin(\Omega n i + \phi_n) e^{-j\Omega m i} =$$

$$\frac{N}{2j} \sum_{n=0}^{\frac{N}{2}} A_n \left[e^{j\phi_n} \delta(m-n) - e^{-j\phi_n} \delta(m - (N-n)) \right], \tag{3}$$

gdzie $\delta(\cdot)$ oznacza deltę Kroneckera oraz $m = 0, 1, \ldots, N-1$.

Liczba linii widma w powyższym wzorze jest równa $N+1$, ponieważ każda z sinusoidalnych składowych wielosinusoidalnego sygnału losowego reprezentowana jest w przedziale częstotliwości względnych $[0, 2\pi)$ przez dwie linie widma (również składowe o częstotliwościach względnych 0 i π). Widmo $U^N(j\Omega m)$ spełnia, dla częstotliwości względnych z przedziału $(\pi, 2\pi)$, warunek:

$$U^N(j(2\pi - \Omega m)) = U^N(-j\Omega m). \tag{4}$$

Korzystając ze wzoru (3) można wyznaczyć periodogram [1] N-elementowej realizacji wielosinusoidalnego sygnału losowego:

$$\Phi_{uu}^N(\Omega m) = \frac{N}{4} \left| U^N(j\Omega m) \right|^2 =$$

$$\frac{N}{4} \left\{ 4A_0^2 \sin^2 \phi_0 \delta(m) + \sum_{n=1}^{\frac{N}{2}-1} A_n^2 \left[\delta(m-n) + \delta(m-(N-n)) \right] + \right.$$

$$\left. 4A_{\frac{N}{2}}^2 \sin^2 \alpha \delta(m - \frac{N}{2}) \right\}, \tag{5}$$

gdzie $m = 0, 1, \ldots, N-1$.

Rozszerzając w definicji (1) zakres zmian chwil czasowych na zakres $i = -\infty, \ldots, -1, 0, 1, \ldots, \infty$ otrzymuje się rozszerzony wielosinusoidalny sygnał losowy $u(i)$. Własności sygnału $u(i)$ wynikające z uśredniania w dziedzinie czasu dla każdej jego realizacji ([8]) przedstawione są w postaci następującego twierdzenia:

Twierdzenie 1. *Jeżeli dany jest rozszerzony wielosinusoidalny sygnał losowy, to:*

1. jego wartość średnia dana jest wzorem:

$$\mathcal{M}\{u(i)\} = A_0 \sin \phi_0; \tag{6}$$

2. jego funkcja autokorelacji dana jest wzorem:

$$R_{uu}(\tau) = A_0^2 \sin^2 \phi_0 + \frac{1}{2} \sum_{n=1}^{\frac{N}{2}-1} A_n^2 \cos(\Omega n \tau) + (-1)^\tau A_{\frac{N}{2}}^2 \sin^2 \alpha, \tag{7}$$

gdzie $\tau = 0, 1, \ldots, \infty$;

3. jego wariancja dana jest wzorem:

$$\sigma^2 = \frac{1}{2} \sum_{n=1}^{\frac{N}{2}-1} A_n^2 + A_{\frac{N}{2}}^2 \sin^2 \alpha. \tag{8}$$

Wartość średnia, periodogram oraz funkcja autokorelacji wielosinusoidalnych sygnałów losowych przyjmują wartości deterministyczne, niezależne od sposobu wyboru rozkładów gęstości prawdopodobieństwa poszczególnych losowych faz. Konsekwencją tej własności jest możliwość dowolnego kształtowania periodogramu lub funkcji autokorelacji poprzez wybór amplitud $\left\{A_0, A_1, \ldots, A_{\frac{N}{2}}\right\}$ składowych sinusoidalnych oraz dwóch deterministycznych faz $\{\phi_0, \alpha\}$. Natomiast losowe fazy są ważnym stopniem swobody w trakcie syntezy wielosinusoidalnych sygnałów losowych. Pozwalają one na kształtowanie tych własności statystycznych sygnałów wielosinusoidalnych, które wynikają z uśredniania po zbiorze wszystkich możliwych realizacji procesu losowego. Na przykład: jeżeli o losowych fazach ϕ_n $(n = 1, 2, \ldots, \frac{N}{2} - 1)$ założy się, że mają jednostajny rozkład gęstości prawdopodobieństwa na odcinku $[0, 2\pi)$, to rozszerzony wielosinusoidalny sygnał losowy jest ergodycznym procesem losowym [8]. Jakakolwiek zmiana rodzaju rozkładu gęstości prawdopodobieństwa losowych faz powoduje, że otrzymany wielosinusoidalny sygnał losowy staje się niestacjonarnym procesem losowym, dla którego wartość oczekiwana $\mathcal{E}\{u(i)\}$ oraz funkcja autokorelacji $\mathcal{E}\{u(i)u(i-\tau)\}$ będą zależne od chwili czasowej i. W przypadku gdy założy się, że $\phi_{\frac{N}{2}}$ jest deterministyczne, a pozostałe fazy mają jednostajny rozkład gęstości prawdopodobieństwa na odcinku $[0, 2\pi)$, to otrzymany wielosinusoidalny sygnał losowy posiada niestacjonarną wartość oczekiwaną:

$$\mathcal{E}\{u(i)\} = A_0 \sin \phi_0 + (-1)^i A_{\frac{N}{2}}^2 \sin \phi_{\frac{N}{2}}. \tag{9}$$

Powyższy warunek niestacjonarności wielosinusoidalnych sygnałów losowych implikuje również ich nieergodyczność. Jest to cecha szczególnie niepożądana, gdy wielosinusoidalny sygnał losowy jest wykorzystywany do symulacji procesów losowych spotykanych w technice, natomiast jest ona szczególnie przydatna w szyfrowaniu danych, ponieważ na podstawie zbioru zaszyfrowanych danych nie można wnioskować o własnościach pojedynczego wyniku szyfrowania i na odwrót.

3. Szyfrowanie danych

Z twierdzenia 1 wynika, że poprzez wybór amplitud $\left\{A_0, A_1, \ldots, A_{\frac{N}{2}}\right\}$ poszczególnych składowych sinusoidalnych oraz dwóch faz $\{\phi_0, \alpha\}$ można w dowolny sposób kształtować periodogram wielosinusoidalnego sygnału losowego. Dodatkowo, zadanemu periodogramowi odpowiada nieskończenie wiele różnych realizacji wielosinusoidalnego sygnału losowego, które różnią się między sobą realizacjami losowych faz. Stanowi to podstawę zaproponowanej metody szyfrowania danych z wykorzystaniem wielosinusoidalnych sygnałów losowych. Algorytm metody składa się z następujących kroków:

1. Ciąg danych o długości M jest dzielony na k podciągów, każdy o długości M_j:

$$\sum_{j=1}^{k} M_j = M, \tag{10}$$

gdzie ciąg liczb $\{M_1, \ldots, M_k\}$ może być jednym z elementów klucza.

2. Używając klasycznych metod szyfrowania [11], kolejne zbiory danych o długości M_j odwzorowywane są w ciąg pomocniczych faz φ_n $(n = 1, 2, \ldots, \frac{N}{2} - 1, N \geq 2M_j + 2)$. Jeżeli $N > 2M_j + 2$, to brakujące fazy można wybrać w sposób dowolny.

   Uzyskane fazy pomocnicze są punktem startowym do generacji realizacji losowych faz ϕ_n $(n = 1, 2, \ldots, \frac{N}{2} - 1)$ wielosinusoidalnego sygnału losowego. Fazy te generuje się wykorzystując klasyczne generatory zmiennych losowych o założonych rozkładach gestości prawdopodobieństwa $\mathcal{F}_n(\varphi_n)$ określonych na zbiorach $\mathcal{S}(\varphi_n)$ $(n = 1, 2, \ldots, \frac{N}{2} - 1)$. Zbiory $\mathcal{S}(\varphi_n)$ powinny być tak wybrane, by spełniały następujące warunki:

   •

$$\mathcal{S}(\varphi_s) \cap \mathcal{S}(\varphi_t) = \emptyset \tag{11}$$

   dla $s \neq t$, $s, t = 1, 2, \ldots, \frac{N}{2}$;

•

$$\mathcal{S}(\varphi_1) \cup \mathcal{S}(\varphi_2) \cup \cdots \cup \mathcal{S}(\varphi_{\frac{N}{2}-1}) \subseteq [0, 2\pi). \tag{12}$$

Z losowej zależności pomiędzy fazami φ_n i ϕ_n wynika, że istnieje nieskończenie wiele różnych możliwych zaszyfrowań tekstu jawnego, które są jednoznacznie deszyfrowywalne.

3. Amplitudy poszczególnych składowych sinusoidalnych wielosinusoidalnego sygnału losowego mogą być dobrane tak, by periodogram sygnału wielosinusoidalnego był równy periodogramowi $\Phi_{vv}(\Omega m T)$ pewnego założonego ciągu danych $v(i)$ $(i = 0, 1, \ldots, N-1)$. Z warunku równości periodogramów:

$$\Phi_{vv}(\Omega m) = \Phi_{uu}^{N}(\Omega m) \tag{13}$$

dla $m = 0, 1, \ldots, \frac{N}{2}$ i zależności (3) otrzymuje się następujący algorytm konstrukcji dyskretnej transformaty Fouriera $U^N(j\Omega m)$ wielosinusoidalnego sygnału losowego:

- dla $m = 0$ oraz $\phi_0 = \frac{\pi}{2}$:

$$U^N(j\Omega m) = \sqrt{N\Phi_{vv}(\Omega m)} + j0; \tag{14}$$

- dla $m = 1, 2, \ldots, \frac{N}{2} - 1$:

$$Re\left\{U^N(j\Omega m)\right\} = \sqrt{N\Phi_{vv}(\Omega m)} \sin\phi_m, \tag{15}$$

$$Im\left\{U^N(j\Omega m)\right\} = -\sqrt{N\Phi_{vv}(\Omega m)} \cos\phi_m, \tag{16}$$

gdzie ϕ_m jest realizacją losowej fazy o rozkładzie gęstości prawdopodobieństwa $\mathcal{F}_m(\varphi_m)$ określonym na zbiorze $\mathcal{S}(\varphi_m)$;

- dla $m = \frac{N}{2}$:

$$U^N(j\Omega m) = \sqrt{N\Phi_{vv}(\Omega m)} \sin\phi_{\frac{N}{2}} + j0, \tag{17}$$

gdzie $\phi_{\frac{N}{2}}$ jest realizacją zmiennej losowej o rozkładzie Bernoulliego $\mathcal{B}\left(\frac{1}{2}, \left\{\frac{\pi}{2}, \frac{3\pi}{2}\right\}\right)$, $(\alpha = \frac{\pi}{2})$;

- dla $m = \frac{N}{2} + 1, \frac{N}{2} + 2, \ldots, N-1$:

$$U^N(j\Omega m) = Re\left\{U^N(j\Omega(N-m))\right\} - jIm\left\{U^N(j\Omega(N-m))\right\}. \tag{18}$$

4. Zaszyfrowany, N-elementowy ciąg danych $u^N(i)$ otrzymuje się w wyniku odwrotnej dyskretnej transformaty Fouriera widma $U^N(j\Omega m)$ przy użyciu algorytmu szybkiej transformacji Fouriera [2].

5. Kroki 3 i 4 algorytmu można powtarzać L-krotnie, przyjmując wygenerowany ciąg $u^N(i)$ jako zbiór faz do wygenerowania kolejnego wielosinusoidalnego ciągu losowego zwiększając każdorazowo czterokrotnie liczbę próbek otrzymywanego sygnału. Brakujące w definicji widma $U^{4N}(j\frac{\Omega}{4}m')$ $(m' = 0, 1, \ldots, 4N-1)$ fazy mogą być generowane dowolnie, jednak w sposób nie powiązany z szyfrowanymi danymi.

W zaproponowanej metodzie szyfrowania danych odtworzenie fazy ϕ_n jest niezależne od przyjętej wartości amplitudy A_n. Z tego spostrzeżenia wynika, że znajomość amplitud nie jest potrzebna, by deszyfrować test jawny, ponieważ w dziedzinie częstotliwości linia widma $U^N(j\Omega m)$ $(m = 0, 1, \ldots, N-1)$ zawiera informację tylko o pojedynczej fazie ϕ_m. Natomiast w dziedzinie czasu pojedyncza faza wpływa na wszystkie wartości $u^N(i)$. Z własności filtracyjnych dyskretnej transformaty Fouriera wynika, że zwiększenie odporności proponowanej metody na mogące się pojawić przypadkowe zakłócenia można osiągnąć poprzez przyporządkowywanie faz poszczególnym składowym sinusoidalnym wielosinusoidalnego sygnału losowego, rozpoczynając od składowych o największych częstotliwościach.

Odporność proponowanej metody na próby łamania można zwiększyć wykorzystując jako jednokierunkową funkcję zapadkową specjalnie zaprojektowany filtr, dla którego:

- można łatwo wyliczyć sygnał wyjściowy po pobudzeniu go wielosinusoidalnym sygnałem losowym,
- bardzo trudno jest zidentyfikować parametry tego filtru bez dodatkowej informacji po to, by móc wyznaczać wartości sygnału pobudzającego. Ta dodatkowa informacja może być również elementem klucza.

4. Przykład

W poniższym przykładzie 32 literom polskiego alfabetu przyporządkowano 32 generatory niezależnych zmiennych losowych o jednostajnych rozkładach gęstości prawdopodobieństwa określonych na rozłącznych przedziałach, które otrzymuje się w wyniku podziału zakresu częstotliwości względnych $[0, 2\pi)$ na 32 odcinki o jednakowej długości. W trakcie szyfrowania nie wprowadzono różnic pomiędzy małymi i dużymi literami alfabetu. Faza reprezentująca i-tą literę alfabetu w trakcie szyfrowania otrzymywana jest jako realizacja zmiennej losowej o jednostajnym rozkładzie gęstości prawdopodobieństwa w zakresie $\frac{2\pi}{32} \pm \frac{2\pi}{64}$.

Do zaszyfrowania wybrano wiersz Jana Lechonia pt. „Poniedziałek" [12]:

Bije dwunasta. Zaczyna się dzień
Mego planety Księżyca.
Wkoło ta sama co zawsze ulica,
Koło mnie codzienny mój cień.

Do domu idę w księżycowej smudze,
Ale to nie mój dom, ja wiem:
Bóg jak do Pawła powie do mnie:
„Twoje życie jest snem,
I ja cię z niego obudzę".

Przed zaszyfrowaniem z tekstu usunięto znaki interpunkcyjne. Na rysunku 1 przedstawiono otrzymany 204-elementowy ciąg realizacji losowych faz, które odpowiadają kolejnym literom wiersza.

W celu zaszyfrowania danych wybrano dla wielosinusoidalnego sygnału losowego okres $N = 512$. Wybór taki spowodował konieczność uzupełnienia zbioru losowych faz o dodatkowe 51 faz, które wygenerowano jako realizacje zmiennej losowej o rozkładzie jednostajnym na odcinku $[0, 2\pi)$. Amplitudy poszczególnych składowych sinusoidalnych sygnału wielosinusoidalnego wybrano tak, by periodogram wielosinusoidalnego sygnału losowego był równy periodogramowi (rys. 4) pewnej 512-elementowej realizacji (rys. 2) białego szumu o rozkładzie normalnym i odchyleniu standardowym 0.30. Unormowaną ocenę autokorelacji tej realizacji, otrzymaną za pomocą estymatora obciążonego, przedstawiono na rys. 3.

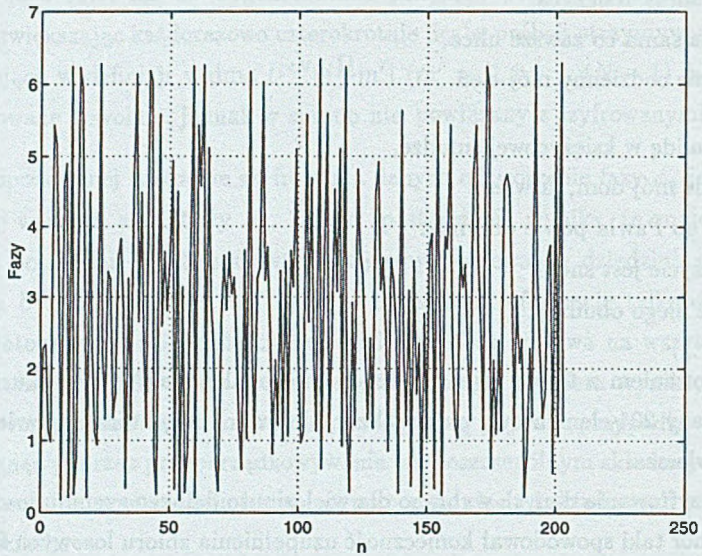
Otrzymaną w wyniku szyfrowania 512-elementową realizację wielosinusoidalnego sygnału losowego przedstawiono na rys. 5. Unormowaną, obciążoną ocenę jego autokorelacji przedstawia rysunek 6. Ocena ta jest identyczna z odpowiednią oceną (rys. 3) wyznaczoną dla wzorcowej 512-elementowej realizacji białego szumu. Z zasady konstrukcji wielosinusoidalnego sygnału losowego wynika, że również periodogram otrzymanego szyfrogramu jest identyczny z periodogramem wzorcowej 512-elementowej realizacji białego szumu.

Powtórzono 100-krotnie powyższą operację szyfrowania, za każdym razem aproksymując periodogram innej 512-elementowej realizacji białego szumu o rozkładzie normalnym.

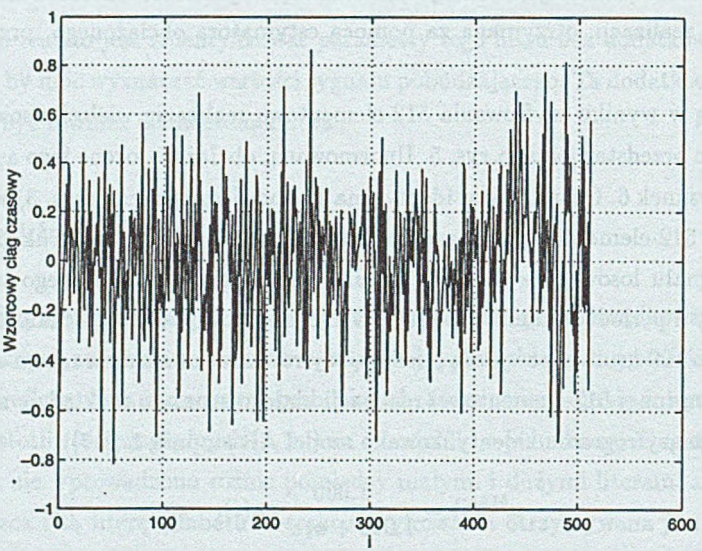
Dla każdego szyfrogramu zidentyfikowano model AR stopnia 1 ([17]):

$$u^{512}(i) = \frac{1.000}{1.000 + a_1 z^{-1}} e(i),$$

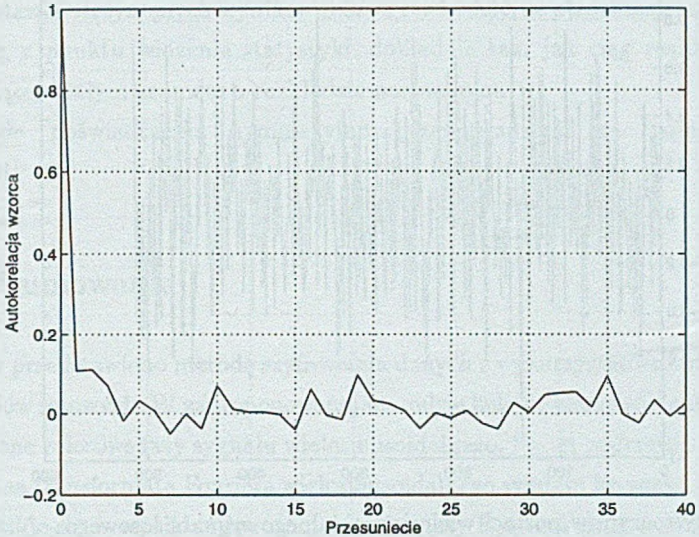
gdzie $e(i)$ jest hipotetycznym białym szumem. Porównując wyniki 100 doświadczeń otrzymano wartość średnią oceny parametru a_1 równą $-2.53 \cdot 10^{-3}$. Natomiast odchylenie standardowe otrzymanych ocen a_1 od średniej wyniosło $4.56 \cdot 10^{-2}$. Wartość ta zgadza się



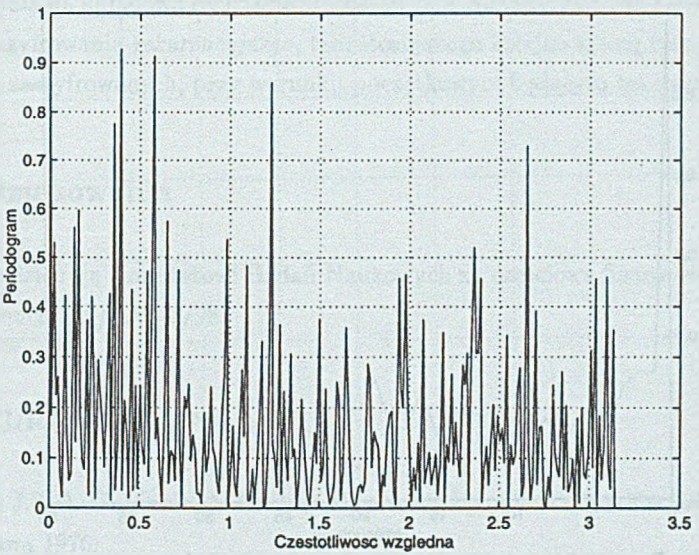
Rys. 1. Ciąg realizacji losowych faz odpowiadających kolejnym literom tekstu jawnego
Fig. 1. The phase-shifts encrypted consecutive characters of plain text



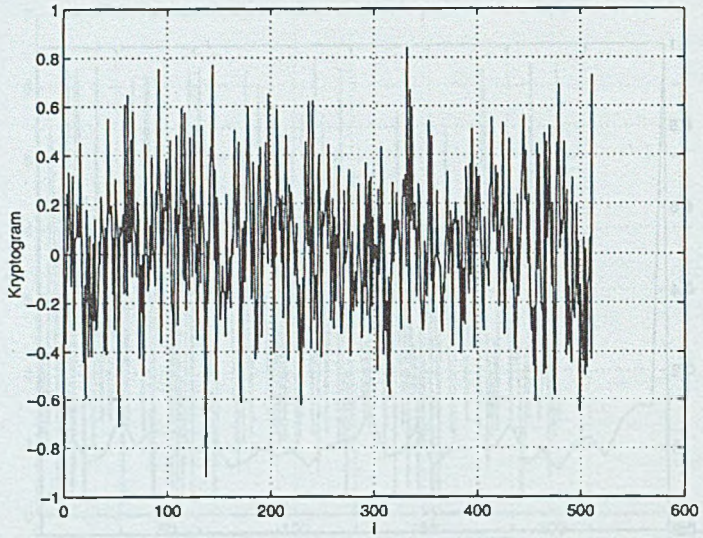
Rys. 2. 512-elementowy ciąg realizacji białego szumu o rozkładzie normalnym
Fig. 2. The 512-sample of normally distributed white noise



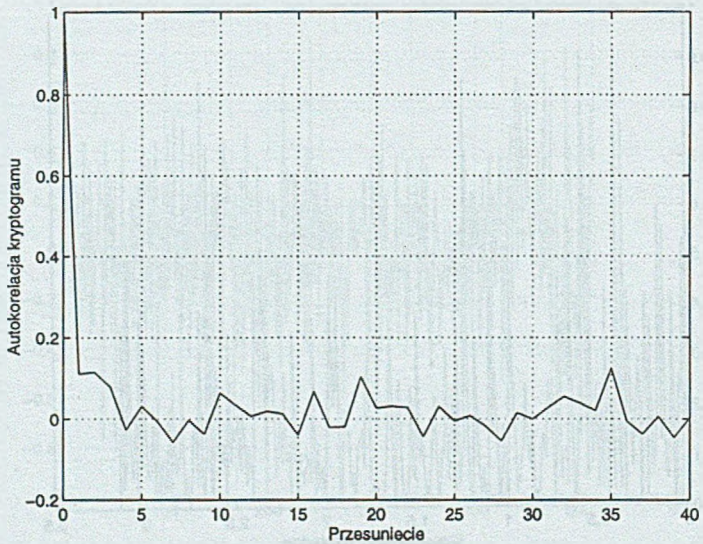
Rys. 3. Obciążona ocena autokorealacji 512-elementowej realizacji białego szumu
Fig. 3. The unbiased autocorrelation estimate of the 512-sample of white noise



Rys. 4. Periodogram 512-elemetowej realizacji białego szumu
Fig. 4. The periodogram of the 512-sample of white noise



Rys. 5. Szyfrogram w postaci wielosinusoidalnego sygnału losowego - $N = 512$
Fig. 5. The encrypted plain text of the form of multisine random signal - $N = 512$



Rys. 6. Obciążona ocena autokoralacji szyfrogramu
Fig. 6. Biased autocorrelation estimate of the encrypted plain text

z dolnym ograniczeniem wynikającym z twierdzenia Cramera-Rao, które dla przypadku $N = 512$ wynosi $4.41 \cdot 10^{-2}$.

Na podstawie otrzymanych wyników można stwierdzić, że otrzymane szyfrogramy zachowują się, z punktu widzenia statystyki, dokładnie tak, jak ciąg realizacji zmiennej losowej będącej białym szumem o rozkładzie normalnym.

Wszystkie doświadczenia symulacyjne przeprowadzono za pomocą systemu MULTI-EDIP [13].

5. Podsumowanie

W pracy przedstawiono metodę szyfrowania danych z wykorzystaniem wielosinusoidalnych sygnałów losowych. W zaproponowanej metodzie kolejne elementy tekstu jawnego są przekształcane w losowe fazy sygnału wielosinusoidalnego. Na tej podstawie konstruowana jest dyskretna transformata Fouriera wielosinusoidalnego sygnału losowego. Zaszyfrowany tekst otrzymuje się w wyniku odwrotnej transformaty Fouriera skonstruowanego widma. Każdy element tego tekstu jest zależny od wszystkich realizacji faz. Dodatkowo, w zaproponowanej metodzie istnieje nieskończenie wiele różnych możliwych zaszyfrowań tekstu jawnego, które są jednoznacznie deszyfrowalne. Rozpowszechnienie procesorów sygnałowych, które umożliwiają bardzo efektywną realizację algorytmu szybkiej transformacji Fouriera, pozwala na układową realizację przedstawionej metody. Metoda nadaje się również dobrze dla szyfrowania *rekurencyjnego*, tzn. stosującego kolejno szereg różnych szyfrowań tekstów już zaszyfrowanych, przy warunku początkowym będącym tekstem jawnym.

6. Podziękowania

Autorzy dziękują Komitetowi Badań Naukowych za częściowe finansowanie niniejszej pracy w ramach BK/RAu-1/98.

LITERATURA

[1] Bendat J.S, A. G. Piersol A. G.: Metody analizy i pomiaru sygnałów losowych. PWN, Warszawa 1976.

[2] Blahut R.E.: Fast Algorithms for Digital Signal Processing. Addison-Wesley Publishing Company, 1984.

[3] Denning D.: Kryptografia i ochrona danych. WNT, Warszawa 1992.

[4] Data encryption standard. Federal Information Processing Standards Publication, page Number 46, Washington 1977. National Bereau of Standards.

[5] Figwer J., Niederliński A.: On the generation of high quality scalar white noise series. Applied Stochastic Models and Data Analysis, 1992, vol. 8, pp. 311–326.

[6] Figwer J., Niederliński A., Kasprzyk J.: A new approach to the identification of linear discrete-time MISO systems. Archives of Control Sciences, 1993, vol. 2 (XXXVIII), No 3–4, pp. 223–239.

[7] Figwer J., Niederliński A.: Using the DFT to Synthesize Multivariate Orthogonal White Noise Series. Transactions of The Society For Computer Simulation, 1995, vol. 12, No. 4, pp. 261–285.

[8] Figwer J.: A new method of random time-series simulation. Simulation Practice and Theory, 1997, vol. 5, No 3, pp. 217–234.

[9] Figwer J.: Multisine Excitation for Process Identification, Archives of Control Sciences, 1996, vol. 5 (XLI), No. 3–4, pp. 279–295.

[10] Goldwasser S., Micali S.: Probabilistic Encryption. Journal of Computer and System Sciences, 1984, vol. 28, pp. 270–279.

[11] Koblitz N.: Wykład z teorii liczb i kryptografii. WNT, Warszawa 1995.

[12] Lechoń J.: Poezje. Zakład Narodowy im. Ossolińskich, Wrocław 1990.

[13] Niederliński A., Kasprzyk J., Figwer J.: MULTI-EDIP analizator wielowymiarowych sygnałów i obiektów. Wydawnictwa Politechniki Śląskiej, Gliwice 1997.

[14] Niederliński A., Figwer J.: Using the DTF to Synthesize Bivariate Orthogonal White Noise Series. IEEE Transactions on Signal Processing, 1995, vol. 43, No. 3, pp. 749–758.

[15] Oppenheim A.V, Schafer R.W.: Digital signal processing. Prentice Hall, Englewood Cliffs, 1975.

[16] Schneider B.: Kryptografia dla praktyków. Protokoły, algorytmy i programy źródłowe w języku C. WNT, Warszawa 1995.

[17] Söderström T., Stoica P.: System Identification. Prentice-Hall International, Hemel Hempstead, U.K., 1988.

Recenzent: Dr inż. Ryszard Maceluch

Wpłynęło do Redakcji 5 grudnia 1997 r.

Abstract

The paper presents basic theorethical foundations of an encryption method based on multisine random time-series. It is proposed to use consecutive characters of the plaintext to generate random phase shifts for all sine components of the multisine random time-series. On this basis the discrete Fourier transform of the corresponding multisine random time-series is constructed. The encrypted plaintext of the form of a multisine random time series is obtained by transforming the discrete Fourier transform into the time-domain. The advantages of the proposed method are as follows:

- for any plaintext there are infinitely many possible encryptions which may be uniquely decrypted;
- each character of the plaintext contributes to all samples of the encrypted plain text, no matter how large is the number of samples;
- plaintext characters being encoded as phase shift bins, and the proposed method is robust with respect to time-series amplitude changes and additive noise;
- silicon implementations of the powerful FFT algorithms in various signal processors, allows swiftly encrypt plaintext and decrypt time-series of any length.

The proposed approach is illustrated by an example in which the verse „Poniedziałek" by Lechoń is encrypted. Obtained results behave like random white noise.