Analiza wybranych parametrów sygnału elektroenergetycznego do kodowania danych przesyłanych w sieciach komputerowych

Piotr Witkowski, Jarosław Zygarlicki
Politechnika Opolska, Wydział Elektrotechniki, Automatyki i Informatyki, Instytut Elektroenergetyki i Energii Odnawialnej, Katedra Inżynierii Biomedycznej, ul. Prószkowska 76 (bud. 2), 45-758 Opole

Streszczenie: W artykule omówiono sposób wyseparowania oraz wykorzystania zmiennych globalnych w czasie, które w przyszłości pozwolą stworzyć unikalny klucz szyfrujący oraz układ szyfrowania danych. Polega on na ciągłej analizie losowego rozkładu zmienności częstotliwości oraz rozwinięciu algorytmów szyfrowania o dodatkowe zabezpieczenie, jakim jest zmieniający się czasie klucz szyfrujący. Celem sprawdzenia, czy opisane rozwiązanie jest możliwe do wykonania, przeprowadzono pomiar napięć w dwóch różnych lokacjach w Polsce. Otrzymany sygnał został wstępnie przefiltrowany celem wygładzenia jego powierzchni. Następnie ustalono dokładne miejsca przecięcia na osi oX metodą przybliżania rozwiązań układów nieokreślonych, po czym otrzymane wartości zostały po raz kolejny przefiltrowane, a otrzymane wyniki poddane analizie, na podstawie której sformułowano wnioski końcowe.

Słowa kluczowe: częstotliwość, sieć elektryczna, kryptografia, szyfrowanie danych, sieć niskiego napięcia

1. Wprowadzenie

Człowiek od zarania dziejów dąży do uniemożliwienia odczytania informacji przez osoby, dla których ich treść nie jest przeznaczona. Już w starożytnym Rzymie dzięki historykowi Swetoniuszowi wiadomo o istnieniu szyfru Cezara, z którego prawdopodobnie korzystał sam Juliusz Cezar. Jest to szyfr należący do szyfrów klasycznych, działających na literach zapisywanych na papierze. Sam szyfr jest prosty i polega na przesunięciu każdej z liter alfabetu o trzy w prawo. Przykład słowo „PAR" zaszyfrowane szyfrem Cezara ma postać „SDU". Celem odtworzenia tego szyfrogramu wystarczy z powrotem przesunąć litery o trzy pozycje w lewo. Szyfr ten powstał w czasach niepiśmiennych, gdzie wykształcenie społeczeństwa było na niskim poziomie, natomiast zastosowanie tego typu rozwiązania współcześnie byłoby stosunkowo proste do odszyfrowania. Powtarzalność liter oraz liczba możliwych kombinacji, nawet uwzględniając zmiany w przełożeniu tekstu czy zamianie na cyfry byłaby niewielka i stosunkowo łatwa do odgadnięcia.

Autor korespondujący:
Piotr Witkowski, piotr.witkowski@doktorant.po.edu.pl

Artykuł recenzowany
nadesłany 07.10.2019 r., przyjęty do druku 04.12.2019 r.

1500 lat po odkryciu szyfru Cezara powstało jego ulepszenie, zwane szyfrem Vigenère'a. Nazwa ta jest błędna, ponieważ pochodzi od nazwiska Blaise de Vigenère, któremu błędnie przypisano autorstwo tego szyfru. Prawdziwym autorem okazał się Giovan Battista Bellaso. Szyfr ten, swego czasu zyskał dużą popularność. Wykorzystywano go podczas toczących się na przełomie lat wojen czy bitew. Modyfikacja szyfru polegała na wprowadzeniu klucza składającego się z przesunięcia wartości umieszczonych w nim liter, zaczynając liczenie od początku alfabetu, czyli od „A", przykładowo: dla litery „D" umieszczonej w kluczu, przesunięcie będzie wynosiło trzy wliczając zero, natomiast dla „S"– osiemnaście. Jeżeli klucz był krótszy niż tekst jawny, wykorzystywano jego wielokrotność. Słowo „PAR" zaszyfrowane kluczem „BC" będzie brzmieć: „QCS". Odszyfrowanie tekstu wymaga znajomości klucza i polega na przesunięciu liter w lewą stronę, czyli wykonania odwrotnej operacji niż ma to miejsce w przypadku szyfrowania. Nie mniej szyfry klasyczne nie są powszechnie uważane za szyfry bezpieczne, bo przez swoją prostotę, niewielką liczbę możliwych kombinacji, moc obliczeniową implementowaną w komputerach klasy PC, złamanie takich szyfrów zajęłoby niewiele czasu [1].

Obecnie stosuje się szyfry bazujące na przesunięciach, zamianie bitów, losowości. Istnieje wiele znanych algorytmów szyfrowania danych opartych na szyfrach symetrycznych, do których można zaliczyć: szyfry blokowe (DES, AES), strumieniowe(implementowane na sprzęt, implementowane na oprogramowanie), a także asymetrycznych: RSA (klucz publiczny i prywatny), szyfrowanie uwierzytelnieniowe, protokół Diffiego-Hellmana (wprowadzający pojęcie szyfrowania kluczem publicznym – 1976 r., wcześniej Ralph Merkle przedstawił pomysł zwany puzlami Mer-

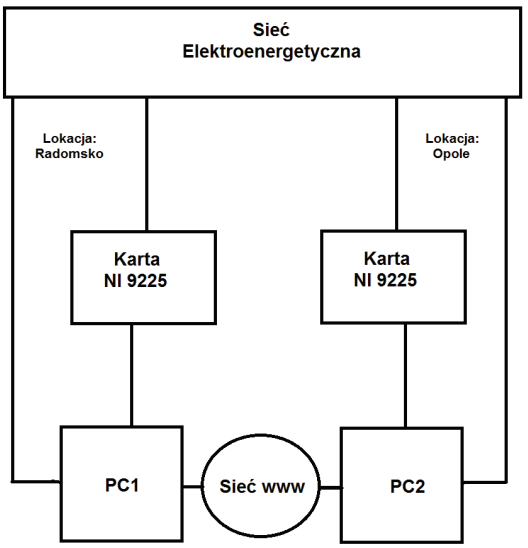
kle'a – 1974 r.) i inne. Coraz częściej przedmiotem dyskusji są założenia związane z szyfrowaniem kwantowym, mającym zapewnić bezpieczeństwo danych w przypadku pojawienia się komputera kwantowego. Dziedziną nauki zajmującą się szyfrowaniem danych, opracowaniem i testowaniem algorytmów szyfrowania jest kryptografia [2].

Podczas tworzenia metod szyfrowania należy zapewnić ich bezpieczeństwo W tym celu należy wziąć pod uwagę szereg czynników – czy klucz będzie jednorazowy czy wielorazowy, czy opracowany algorytm będzie odporny na modele ataku typu czarna skrzynka (COA, KPA, CPA, CCA) czy szara skrzynka (atak bocznym kanałem, ataki inwazyjne). Określenie kategorii bezpieczeństwa (uwzględniając podstawowe cele bezpieczeństwa, jakimi są nierozróżnialność – IND i niereformowalność – NM) w połączeniu z modelami ataków, np. kategoria IND-CPA, czyli tzw. bezpieczeństwo semantyczne. To tylko niektóre z wielu czynników, które musi uwzględnić kryptograf opracowujący nowy algorytm lub metodę szyfrowania danych [1, 4].

Obecnie trwają prace nad nowymi sposobami oraz metodami szyfrowania. Jedną z propozycji jest metoda generowania klucza za pomocą informacji pobieranych z sieci elektroenergetycznej, gdzie sygnał występujący w sieci opisany jest za pomocą sinusoidy [3]. W rzeczywistości w sygnale elektroenergetycznym występuje szereg zjawisk, które powodują zakłócenia w postaci: wolnych zmian napięć, szybkich zmian napięć, zapadów napięcia, krótkich przerw w zasilaniu, długich przerw w zasilaniu, flickerów (fluktuacji napięcia), przepięć, przepięć szpilkowych i innych. Poza wymienionymi zakłóceniami występują fluktuacje częstotliwości harmonicznej. Fluktuacje te mają charakter stochastyczny i mogą być wykorzystane podczas procesu szyfrowania danych, ponieważ propagują się globalnie. Parametry sieci elektroenergetycznej regulują normy. W Europie głównym tego typu dokumentem jest norma EN 50160 określająca dopuszczalne wartości mogące występować w sieci elektroenergetycznej [6].

W pracy wykorzystano element, który w większości przypadków jest elementem niepożądanym, tj. zmiany częstotliwościowe [7]. Na ich podstawie podjęto próbę stworzenia indywidualnego klucza szyfrującego [5], tym samym wzmocnienia skuteczności algorytmów szyfrowania danych. Celem sprawdzenia, czy proponowane rozwiązanie jest wykonalne i ma realną szansę na fizyczną implementację przeprowadzono badanie, którego przebieg oraz wyniki zostały przedstawione w artykule.

Rys. 1. Karta National Instruments NI 9225 podczas pomiaru napięć. Wraz z kartą do podstawki podłączone są karty NI 9227 oraz NI 9401, które nie zostały wykorzystane podczas niniejszego badania
Fig. 1. Presentation of the National Instruments NI 9225 card during voltage measurement together with the card, the NI 9227 and NI 9401 cards that are not used during this test are connected to the base



Rys. 2. Schemat podłączeń urządzeń pomiarowych uwzględniający obie lokacje
Fig. 2. Connection diagram for measuring devices including both locations

2. Lokacja punktów pomiarowych

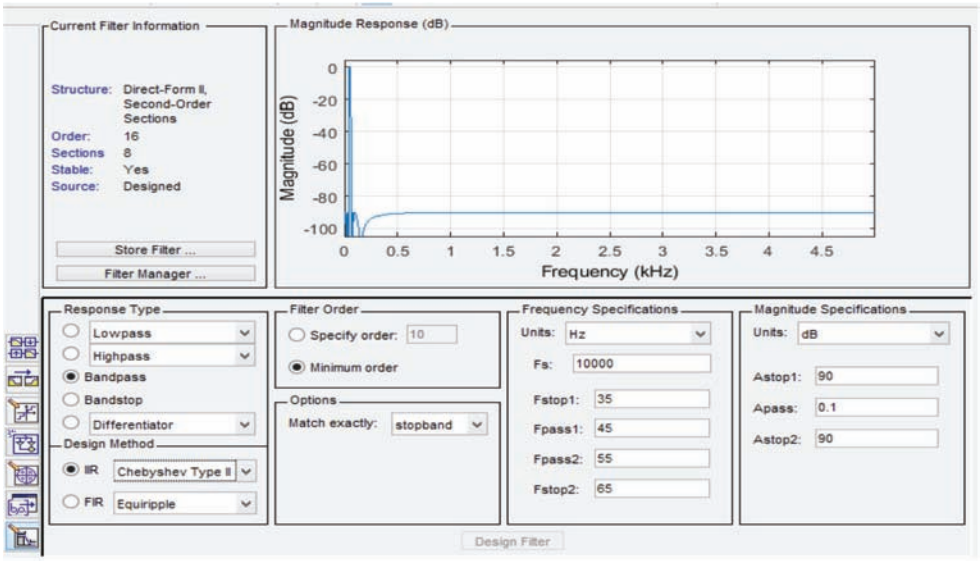
Działania rozpoczęto od przeprowadzenia pomiarów napięć panujących w sieci elektroenergetycznej niskiego napięcia. Do rejestracji przeprowadzonych pomiarów wybrano kartę National Instruments NI 9225 (rys. 1). Dobór karty wynikał z jej specyfikacji. Karta jest wyposażona w trójkanałowy moduł wejściowy, umożliwiający szeroki zakres pomiarów, m.in. monitorowanie jakości energii oraz analizę stanów przejściowych i harmonicznych z jednoczesnym próbkowaniem z dużą prędkością. Ponadto można ją zastosować podczas pomiarów wysokich napięć, parametrów silnika czy akumulatorów. Karty rozmieszczono w dwóch lokacjach oddalonych od siebie o 120 km. Koniecznym wymogiem było, aby lokacje znajdowały się w tej samej sieci elektroenergetycznej ze względu na panującą w niej częstotliwość. Na obszarze Unii Europejskiej częstotliwość jest parametrem określonym w normie EN 50160 i wynosi 50 Hz. Pierwszą lokacją było Opole, kolejną Radomsko.

Na rysunku 2 przedstawiono schemat stanowiska pomiarowego. Karty NI 9225 wraz komputerami klasy PC (PC1 oraz PC2) były podłączone do sieci elektroenergetycznej niskiego napięcia. Komputery odpowiadały za przetwarzanie oraz archiwizację zarejestrowanych przez kartę danych, były również podłączone do sieci WWW, co umożliwiało komunikację czy transfer zarejestrowanych danych. Pomiary napięć trwały około tygodnia i oba napięcia mierzone były w tym samym czasie. Zebrane dane skonwertowano do postaci macierzowej w środowisku MATLAB, a następnie poddano je analizie oraz wyodrębniono i porównano zmienne globalne w czasie z obu lokacji, co zostało zaprezentowane w kolejnym rozdziale.

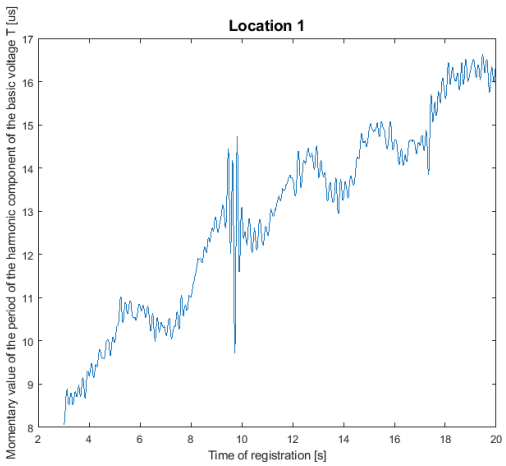
3. Przetwarzanie i analiza zebranych danych

Pierwszym etapem akwizycji zebranych danych było wygładzenie powierzchni sygnałowej sygnałów z obu lokacji. W tym celu, za pomocą oprogramowania Filter Design & Analysis Tool środowiska obliczeniowego MATLAB, zaprojektowano filtr pasmowo-przepustowy pierwszego rzędu, którego specyfikacja została przedstawiona na rys. 3.

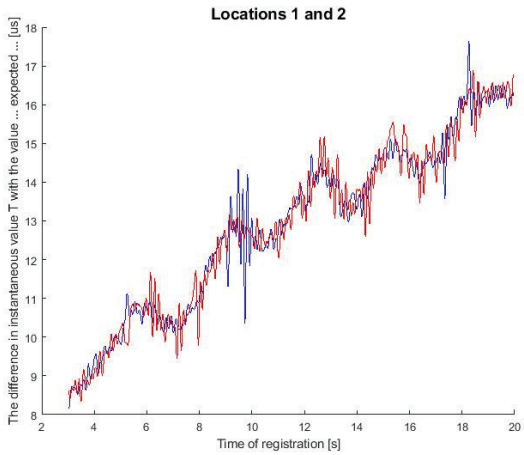
Aby możliwa była analiza częstotliwościowa, należało zacząć od estymacji miejsc przecięcia sygnału z osią oX. W oparciu o metodę najmniejszych kwadratów zaprojektowano funk-



Rys. 3. Projekt filtra pasmowo-przepustowego użytego do wygładzenia powierzchni sygnału z przedstawionymi jego parametrami jak: wartości w paśmie przepustowym oraz zaporowym, częstotliwością czy typem filtra
Fig. 3. Design of the bandpass filter used to smooth the signal surface with its parameters such as: values on the band and dam band, frequency and type of filter



Rys. 4. Chwilowa wartość okresu składowej harmonicznej napięcia podstawowego T, otrzymana w wyniku działania funkcji bazującej na MNK
Fig. 4. The momentary value of the time period of the harmonic component of the basic voltage T, obtained by a function based on MNK

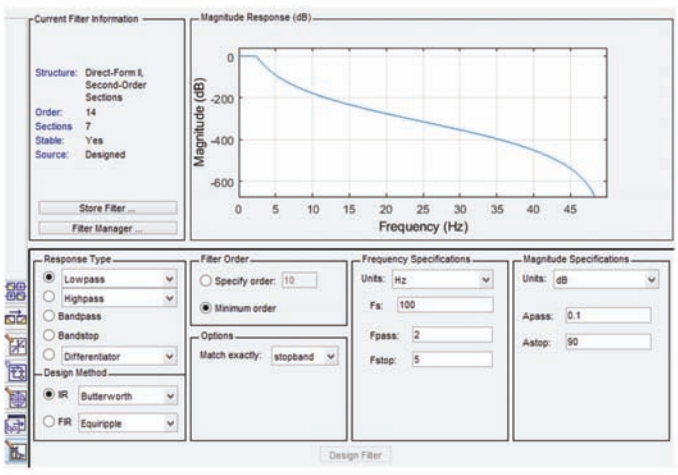


Rys. 5. Zestawienie wykresów z obu lokacji – wyraźny brak jakiejkolwiek korelacji
Fig. 5. Comparison of charts from both locations – a clear lack of any correlation

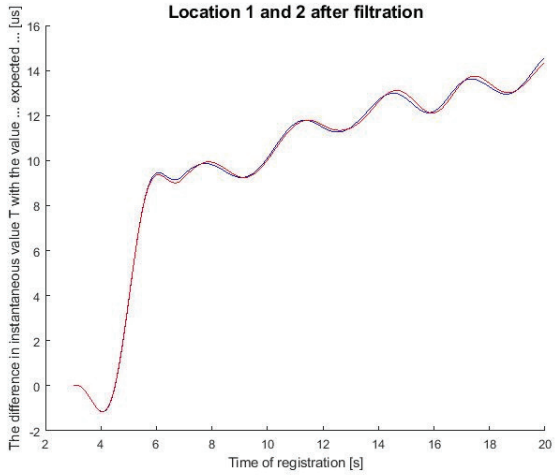
cję, która pozwoliła wyseparować miejsca przecięcia z osią 0. Użycie funkcji MNK posłużyło do obliczeń chwilowej wartości okresu składowej harmonicznej podstawowej napięcia jej graficzna implementacja została przedstawiona na rys. 4. Następnie zestawiono ze sobą wykresy z obu lokacji. Na tym etapie badania zaobserwowano brak korelacji między wygenerowanymi wykresami (rys. 5).

Kolejnym krokiem było zaprojektowanie filtru drugiego rzędu (rys. 6.) z wartościami dobranymi w sposób empiryczny. Podczas projektu filtru kluczowe jest dobranie jego parametrów, gdyż dzięki temu możliwe będzie uzyskanie korelacji między zmiennymi.

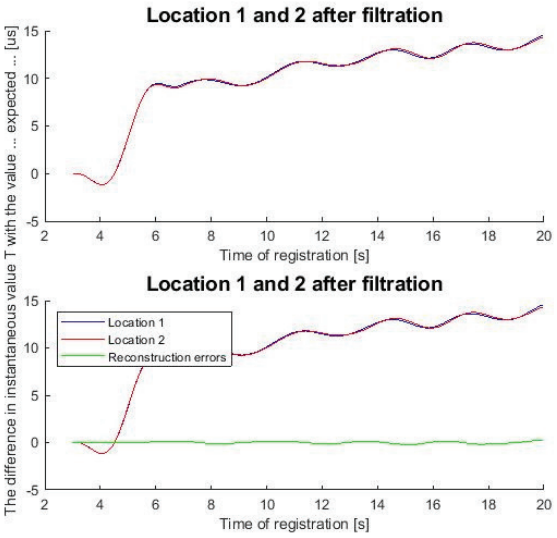
Po przefiltrowaniu oba wykresy zostały zestawione na rys. 7. W wyniku otrzymano korelację z niewielkimi odchyleniami w części zaporowej. Punkty, w których uzyskano korelację można wykorzystać jako generator liczb losowych. Wykorzystywanym tu parametrem sieci elektroenergetycznej jest częstotliwość, co umożliwia stworzenie klucza częstotliwościowego zmiennego w czasie. Może on zostać wykorzystany jako wzmocnienie (wsparcie) obecnie działających algorytmów szyfrowania danych. Badanie powtórzono dla innych pomiarów uzyskując



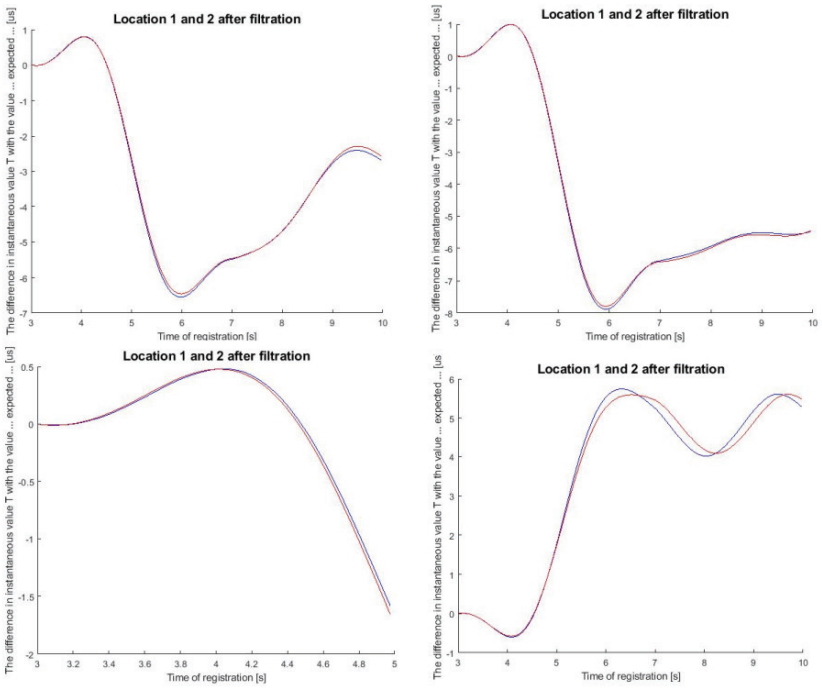
Rys. 6. Projekt filtru drugiego rzędu z przedstawionymi parametrami – wartości na paśmie przepustowym oraz zaporowym, częstotliwością czy typem filtra
Fig. 6. The design of the second order filter with the presented parameters such as values on the pass and dam band, frequency or type of filter



Rys. 7. Po przefiltrowaniu otrzymanych wyników uzyskano korelację z odchyleniem w części zaporowej
Fig. 7. The results obtained after filtering correlated with the deviation in the dam part



Rys. 9. Otrzymane wyniki po przefiltrowaniu wraz z błędami rekonstrukcji przedstawionymi w formie graficznej
Fig. 9. The results obtained after filtering together with reconstruction errors presented in graphic form



Rys. 8. Powtórzone badania dla czterech przykładowych pomiarów – we wszystkich można zaobserwować korelację oraz odchylenie w części zaporowej
Fig. 8. Repetition of the test for other measurements, presenting four examples in all can be observed correlation and deviation in the dam

wyniki przedstawione na rys. 8. Obliczono występujące błędy rekonstrukcji, które w formie graficznej przedstawiono na rys. 9. Aby lepiej zobrazować cały zachodzący proces od momentu rejestracji parametrów pobranych z sieci elektroenergetycznej do momentu uzyskania generatora liczb losowych stworzono algorytm przedstawiony na rys. 10.

4. Wnioski

W wyniku przeprowadzonego badania osiągnięto korelację z widocznymi na rys. 9 błędami rekonstrukcji. Błędy te można zmniejszyć przez zmianę parametrów filtra drugiego rzędu. Z przeprowadzonego badania wynika, iż jest możliwe wygenerowanie oraz implementacja klucza bazującego na fluktuacji częstotliwościowej, występującej w sygnale sinusoidalnym napięcia w sieci elektroenergetycznej. W różnych lokacjach tej samej sieci elektroenergetycznej istnieje możliwość, przez odpowiednie zastosowanie filtrów, doprowadzenia do korelacji między wartościami chwilowymi T i wykorzystania ich jako klucza do stworzenia szyfrogramu przesyłanego siecią globalną, przesłania go odbiorcy i przekształcenia w tekst jawny za pomocą klucza częstotliwościowego jednokrotnego użytku, będącego wsparciem dla obecnie znanych algorytmów szyfrowania danych.

Rys. 10. Przedstawienie procesu obrazującego akwizycję sygnału i działanie generatora
Fig. 10. Presentation of the process illustrating the operation and acquisition of the generator

Projekt obecnie jest rozwijany. W ciągu dwóch lat planuje się jego zakończenie. W ramach dalszych prac związanych z realizacją projektu planuje się stworzenie fizycznego kodera oraz dekodera, zbierającego informacje z sieci elektroenergetycznej, komunikującego się z komputerem klasy PC, stworzenie oprogramowania umożliwiającego przetwarzanie, szyfrowanie i rozszyfrowanie danych wspomaganego przez obecnie istniejące algorytmy bazujące na kluczu częstotliwościowym.

Bibliografia

1. Aumasson J.-P., *Nowoczesna kryptografia praktyczne wprowadzenie do szyfrowania* Wydawnictwo PWN, Warszawa 2018, ISBN 978-83-01-19900-5.
2. Karbowski M., *Podstawy Kryptografii* (Wyd. III) Wydawnictwo: Helion, Gliwice 2014, ISBN: 978-83-246-6975-2.
3. Marzecki J., Pawlicki B., *Kształtowanie obciążeń u odbiorców końcowych w oparciu o częstotliwość napięcia zasilającego*, „Przegląd Elektrotechniczny", R. 90, Nr 1, 2014, 182–185.
4. Ratnadewi, Roy PramonoAdhie, Yonatan Hutama, A. Saleh Ahmar, M I Setiawan, *Implementation Cryptography Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES) Method in Communication System Based Near Field Communication (NFC)*, "Journal of Physics: Conference Series", Vol. 954, 2009, DOI: 10.1088/1742-6596/954/1/012009.
5. Zhe Liu, Kim-Kwang Raymond Choo, Johann Grossschadl, *Securing Edge Devices in the Post-Quantum Internet of Things Using Lattice-Based Cryptography*, "IEEE Communications Magazine", Vol. 56, Issue 2, 2018, 158–162, DOI: 10.1109/MCOM.2018.1700330.
6. Kaczmarek M., *Próba określenia dokładności transformacji sygnałów sinusoidalnych o częstotliwościach 50 Hz* i wyższych przez przekładniki napięciowe, „Przegląd Elektrotechniczny", R. 88, Nr 11b, 2012, 233–236.
7. Zieliński T.P., *Cyfrowe przetwarzanie sygnałów. Od teorii do zastosowań*, Wydawnictwo WKŁ, Warszawa 2005, ISBN 83-206-1596-8.

Analysis of Selected Power Signal Parameters for Coding Data Transfer in Computer Networks

Abstract: The article discusses the way of separating and using global variables in time, which in the future will create a unique encryption key and data encryption system. It is based on continuous analysis of the random distribution of frequency variability and the development of encryption algorithms with the additional security, which is the changing time key encryption. In order to check whether the described solution is feasible, voltage measurements were carried out in two different locations in Poland. The received signal was pre-filtered to smooth its surface. Then the exact intersection points were determined on the oX axis by the method of approximation of solutions of indeterminate systems, after which the obtained values were once again filtered and the results obtained were analyzed, on the basis of which final conclusions were formulated.

Keywords: frequency, electrical grid, cryptography, data encryption, low voltage network

mgr inż. Piotr Witkowski
piotr.witkowski@doktorant.po.edu.pl
ORCID: 0000-0002-2293-6462

Absolwent Wydziału Elektrotechniki, Automatyki i Informatyki, Politechniki Opolskiej na kierunku Informatyka. W latach 2017–2019 właściciel serwisu zajmującego się naprawą komputerów i elektroniki użytkowej AllByte System w Radomsku. Obecnie doktorant I roku studiów III stopnia na kierunku: Elektrotechnika Wydziału Elektrotechniki, Automatyki i Informatyki, Politechniki Opolskiej. Zainteresowania naukowe: przetwarzanie sygnałów, informatyka śledcza, obserwacja zjawisk zachodzących podczas procesów związanych z lutowaniem BGA.

dr hab. inż. Jarosław Zygarlicki, prof. PO
j.zygarlicki@po.opole.pl
ORCID: 0000-0001-9330-4369

Urodził się w 1978 r. w Brzegu. Ukończył studia w 2002 r. na Wydziale Elektroniki Politechniki Wrocławskiej. W latach 2002–2008 zatrudniony jako asystent na Wydziale Elektrotechniki, Automatyki i Informatyki Politechniki Opolskiej. W latach 2008–2014 zajmował stanowisko adiunkta. Od 2014 r. profesor uczelni w Politechnice Opolskiej. Zainteresowania badawcze to cyfrowe przetwarzanie sygnałów, ze szczególnym uwzględnieniem analiz dotyczących jakości energii elektrycznej.