Appl. Math. and Comp. Sci., 1998, Vol.8, No.3, 657–670

DATA ENCRYPTION USING N-LAG WHITE MULTISINE RANDOM TIME-SERIES

ANTONI NIEDERLIŃSKI*, JAROSŁAW FIGWER*

A new data encryption method based on N-lag white multisine random time-series (WMRTS) is presented. Its essence is that consecutive characters of the cleartext are used to generate phase shifts for all or for some of the sine components of an N-lag WMRTS. This time-series is defined in the frequency domain by its Discrete Fourier Transform (DFT). It consists of two spectra: the phase-shift spectrum containing encrypted characters and the amplitude spectrum with the same amplitude for all frequencies. This DFT is calculated with the help of the Fast Fourier Transform (FFT) algorithm transformed into the time domain. The result is the cyphertext in the form of an N-lag WMRTS. To decrypt the cyphertext, it is processed by the FFT algorithm, the result being the original DFT, from which all phase shifts are recovered. The paper presents theoretical foundations of the method and a numerical example demonstrating its effectiveness.

1. Introduction

There is a close connection between white noise generation and data encryption. The essence of this connection is that a number of popular data encryption methods work on the principle of adding the cleartext characters bit-by-bit modulo 2 to elements of random (possibly uncorrelated) time-series (Denning, 1983; Des, 1977; Koblitz, 1994; Schneider, 1994). The role played by the random addendum is to remove from the cyphertext any correlation.

The approach proposed in this paper is different, the idea being to embed the cleartext directly into an N-lag white multisine random time-series (WMRTS). Precisely, this embedding is done into its frequency-domain representation, namely its phase-shift spectrum. This spectrum together with a properly chosen amplitude spectrum are next transformed into the time-domain, giving the cyphertext. It is therefore both a *deep embedding* (the characters being hidden in the frequency model of the cyphertext) and a *broad embedding* (the contribution of any character of the cleartext is dispersed over all the samples of the cyphertext).

The idea originated from a recently published method of white noise modelling by means of multisine random time-series (MRTS) (Figwer and Niederliński, 1992; 1995; Niederliński and Figwer, 1995). The method aims at making an N-sample MRTS

* Institute of Automation, Silesian Technical University, ul. Akademicka 16, 44–100 Gliwice, Poland, e-mail: {aniderlinski,jfigwer}@ia.polsl.gliwice.pl.

simulate white noise by defining the MRTS in a suitable way in the frequency domain. The cornerstone of this definition is (obviously) a flat power spectral density (PSD). To go ahead with the synthesis, the PSD has to be converted into a DFT which is in turn transformed by the FFT into its time-domain representation. This time-domain representation behaves exactly like white noise for the correlation function lags not exceeding N. Hence it is referred to as the N-lag white multisine random time-series (WMRTS).

However, any PSD (including those for WMRTS's) is a real-number frequency characteristic, which corresponds to an infinite number of complex-number DFT frequency characteristics, each given in terms of a different phase-shift spectrum and the same (flat) amplitude spectrum. This arbitrariness of the phase-shift spectrum may be used for a number of purposes, e.g. for designing into the WMRTS a small crest factor in case the WMRTS is used as an excitation signal for system identification, see (Figwer *et al.*, 1993).

The arbitrariness of the phase-shift spectrum may also be used to make it represent characters of some cleartext without distorting the whiteness of the N-lag WMRTS. As a result, no correlation whatever may be detected in the N-lag WMRTS despite it being the cyphertext.

It should be emphasized that even if the phase shifts used are slightly correlated, the N-lag WMRTS autocorrelation function looks for lags up to N exactly like a white-noise autocorrelation function: the requirement of a constant PSD amplitude is somehow enhancing the *randomness* of the N-lag WMRTS when compared with the *randomness* of the phase-shift spectrum.

The mathematical techniques used in the sequel are simple and standard in digital signal processing. The readers missing details are referred to (Bendat and Piersol, 1986; Nussbaumer, 1982; Oppenheim and Schafer, 1975).

The paper is organized as follows. In Section 2, the MRTS's are defined and their properties are presented. Section 3 is intended to introduce N-lag WMRTS's. It is proposed to generate such time-series from their PSD representation using the inverse Discrete Fourier Transform as implemented by any FFT algorithm. It is further demonstrated that N-lag WMRTS's have autocorrelation functions for the first N lags exactly like white noise. In Section 4, the encryption mechanism is presented in detail, special attention being paid to those of its aspects, which differ from standard encryption procedures. Section 5 discusses the decryption mechanism. Section 6 is devoted to the study of an example of using the method to encrypt a well-known Shakespearean quotation. In Section 7, possible variations of the presented method are discussed.

2. Multisine Random Time-Series

Definition 1. The *N-sample MRTS* is defined (for N even) in the time-domain by a sum of $N/2+1$ discrete-time harmonic sines including a constant component:

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

where $\Omega = 2\pi/N$ denotes the fundamental relative frequency, $n = 0, 1, \ldots, N/2$ is used to label the consecutive harmonics of this frequency in the range $[0, \pi]$, $i = 0, 1, \ldots, N-1$ denotes the consecutive discrete time instants, A_n are the deterministic amplitudes of sine components ($A_n \in \mathcal{R}$), ϕ_n are phase shifts of which ϕ_0 and $\phi_{N/2}$ are deterministic and the remaining phase shifts are random, independent and arbitrarily distributed on a subset of $[0, 2\pi)$.

The N-sample MRTS can be defined in the frequency-domain by its N-point discrete Fourier transform $U^N(j\Omega m)$, referred to as the spectrum. It is determined as follows:

$$\begin{aligned} U^N(j\Omega m) &= \sum_{i=0}^{N-1} u^N(i) e^{-j\Omega mi} = \sum_{i=0}^{N-1} \sum_{n=0}^{N/2} A_n \sin(\Omega ni + \phi_n) e^{-j\Omega mi} \\ &= \sum_{n=0}^{N/2} \frac{A_n}{2j} \left[e^{j\phi_n} \sum_{i=0}^{N-1} e^{j(\Omega n - \Omega m)i} - e^{-j\phi_n} \sum_{i=0}^{N-1} e^{-j(\Omega n + \Omega m - 2\pi)i} \right] \\ &= \frac{N}{2j} \sum_{n=0}^{N/2} A_n \left[e^{j\phi_n} \delta(m-n) - e^{-j\phi_n} \delta\big(m - (N-n)\big) \right] \end{aligned} \tag{2}$$

where $\delta(\cdot)$ is the Kronecker delta function and

$$\sum_{i=0}^{N-1} e^{-j\Omega ki} = \begin{cases} N & \text{if } k = 0, N, \ldots \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

The number of the relative frequencies included in $U^N(j\Omega m)$ is N. The frequencies 0 and $\Omega N/2$ are represented by double-length lines. Additionally, the spectrum $U^N(j\Omega m)$ of a real-valued MRTS satisfies the condition

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

The following lemma presents some properties of MRTS's (see (Figwer, 1997) for details) which follow from time-domain averaging on any particular time-series realization:

Lemma 1. *Consider an N-sample MRTS as given by Definition 1. Its properties are as follows:*

1. *The periodogram is given by*

$$\begin{aligned} \Phi_{uu}^N(\Omega m) &= \frac{TN}{4} \left| U^N(j\Omega m) \right|^2 \\ &= \frac{TN}{4} \left\{ 4A_0^2 \sin^2 \phi_0 \delta(m) + \sum_{n=1}^{N/2-1} A_n^2 \left[\delta(m-n) + \delta\big(m - (N-n)\big) \right] \right. \\ &\quad \left. + 4A_{N/2}^2 \sin^2 \phi_{N/2} \delta\left(m - \frac{N}{2}\right) \right\} \end{aligned} \tag{5}$$

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

2. *The autocorrelation function is given by*

$$R_{uu}(\tau) = \frac{1}{N}\sum_{m=0}^{N-1} \Phi_{uu}^{N}(\Omega m) e^{j\Omega m\tau}$$

$$= A_0^2 \sin^2\phi_0 + \frac{1}{2}\sum_{n=1}^{N/2-1} A_n^2 \cos(\Omega n\tau) + (-1)^{\tau} A_{N/2}^2 \sin^2\phi_{N/2} \quad (6)$$

where $\tau = 0, 1, \ldots, \infty$.

3. *The mean value is given by*

$$\mathcal{M}\{u(i)\} = \sum_{i=0}^{N-1} u^N(i) = A_0 \sin\phi_0 \quad (7)$$

4. *The variance is given by*

$$\sigma^2 = R_{uu}(0) - \left[\mathcal{M}\{u(i)\}\right]^2 = \frac{1}{2}\sum_{n=1}^{N/2-1} A_n^2 + A_{N/2}^2 \sin^2\phi_{N/2} \quad (8)$$

It should be noticed that in spite of the random phase shifts ϕ_n for $n = 1, 2, \ldots, \phi_{N/2-1}$, the periodogram and autocorrelation functions obtained using time-domain averaging are *deterministic*, real-valued functions. The *determinism* is due to the fact that the dependence of $u^N(i)$ on the random phase shifts has been averaged out of those functions.

This implies in turn that by properly choosing the set of deterministic amplitudes $\{A_0, A_1, \ldots, A_{N/2}\}$ and two deterministic phases $\{\phi_0, \phi_{N/2}\}$, the shape of the MRTS periodogram (or autocorrelation function) can be fitted to any predetermined PSD function (or autocorrelation function), including those of white noise.

Of course, the random phase shifts ϕ_n for $n = 1, 2, \ldots, \phi_{N/2-1}$ are eventually needed to synthesize the time-series with predetermined PSD or autocorrelation properties. Those random phase shifts are important degrees of freedom for the WMRTS synthesis and may be determined to satisfy a number of goals. In the present paper they are used to hold information about encrypted characters of the cleartext.

3. N-Lag White Multisine Random Time-Series

If the PSD of white noise is approximated by the periodogram of an N-sample MRTS (Figwer and Niederliński, 1992; 1995), the resulting time-series $w(i)$, referred to as the N-lag Multisine Random White Time-Series (N-lag WMRTS), has an autocorrelation function which, for lags $\tau = 0, 1, \ldots, N-1$, is the same as the white noise autocorrelation function. This is the essence of the following lemma.

Lemma 2. *Consider an N-sample MRTS as given by Definition 1 and assume that the deterministic parameters of its sine components are chosen as follows:*

- *amplitudes $A_n = A$ for $n = 1, 2 \ldots, N/2 - 1$, $A_0 = A_{N/2} = A/2$;*
- *phase shifts ϕ_0 and $\phi_{N/2}$ are equal to $\pi/2$.*

Then the resulting N-lag WMRTS has the following properties:

1. *Its periodogram is given by*

$$\Phi_{ww}^{N}(\Omega m) = \frac{NA^2}{4} \sum_{n=0}^{N-1} \delta(m-n) \tag{9}$$

2. *Its autocorrelation function is given by*

$$R_{ww}(\tau) = \begin{cases} NA^2/4 & \text{if } \tau = 0 \\ 0 & \text{if } 1 \leq \tau < N \end{cases} \tag{10}$$

We emphasize that characteristic features of whiteness such as a flat spectrum and the autocorrelation function equal zero for all lags but 0, appear only for N-sample realizations of N-lag WMRTS's.

For a predetermined value A, predetermined phase shifts $\phi_0 = \phi_{N/2} = \pi/2$ and predetermined distributions of the remaining phase shifts, the procedure for obtaining N-samples of N-lag WMRTS's is based on efficient FFT algorithms. This procedure consists of two steps:

Step 1. The synthesis of the N-lag WMRTS spectrum $U^N(j\Omega m)$:

- for $m = 0$:

$$W^N(j0) = N\frac{A}{2} + j0 \tag{11}$$

- for $m = 1, 2, \ldots, N/2 - 1$:

$$\mathrm{Re}\left\{W^N(j\Omega m)\right\} = \frac{N}{2} A \sin\phi_m \tag{12}$$

$$\mathrm{Im}\left\{W^N(j\Omega m)\right\} = -\frac{N}{2} A \cos\phi_m \tag{13}$$

where ϕ_m are random, independent and arbitrarily distributed;

- for $m = N/2$:

$$W^N(j\pi) = N\frac{A}{2} \sin\phi_{N/2} + j0 \tag{14}$$

where $\phi_{N/2}$ is deterministic;

- for $N - m = N - 1, N - 2, \ldots, N - (N/2 - 1)$:

$$W^N(j\Omega(N-m)) = \mathrm{Re}\left\{W^N(j\Omega m)\right\} - j\mathrm{Im}\left\{W^N(j\Omega m)\right\} \tag{15}$$

Step 2. The transformation of the N-lag WMRTS spectrum $W^N(j\Omega m)$ into the time-domain by using any powerful FFT algorithm (Nussbaumer, 1982). This results in an N-sample N-lag WMRTS.

4. Encrypting the Cleartext into an N-Lag WMRTS

The N-lag WMRTS data encryption method advocated in this paper may be reduced to the following basic stages, within which some obvious variations are possible:

1. At the first stage:

   - We call the number of characters in a given cleartext the *length* of this cleartext. The cleartext series of length L is divided into k subseries of length L_j each, $\sum_{j=1}^{k} L_j = L$. Each L_j is bounded from above by an even number N_j, $L_j \leq N_j$. The sequence of integers

     $$\{L_1, \ldots, L_k, N_1, \ldots, N_k\}$$

     is treated as the *first key sequence.*

   - Assume that the cleartext alphabet contains $M \leq L$ different kinds of characters. The entire interval $[0, 2\pi)$ of possible phase shifts φ is divided into M not overlapping subintervals $S_m(\varphi) = [\varphi_{m,\min}, \varphi_{m,\max})$, $m = 1, 2, \ldots, M$. As a result, a *one-to-one* mapping $\varphi \to S_m(\varphi)$ follows, which assigns to any phase shift φ one and only one subinterval $S_m(\varphi)$.

   - To any kind of character C_m, $m = 1, 2, \ldots, M$ of the cleartext alphabet a unique subinterval $S_m(\varphi)$ is assigned. As a result, a *one-to-one* mapping

     $$C_m \to S_m(\varphi), \quad m = 1, 2, \ldots, M$$

     follows. This mapping is considered as the *second key sequence.*

     The subintervals $S_m(\varphi)$ may be of equal length or their lengths may depend on the relative frequency of the assigned character C_m in the cleartext.

     The assignment of *characters* to *intervals* contributes to enhanced robustness against noise as compared with an encryption method based on some *Point* $\to$ *Point* principles, *Point* being a character, a bit, a byte etc.

   - To any subinterval $S_m(\varphi)$ a probability density function $\mathcal{F}_m(\varphi)$ is assigned. These density functions may be chosen freely, e.g. as uniform probability density functions (see example).

2. At the second stage, all the cleartext subseries are considered in turn. For any character $C_{j,n}$, $n = 1, 2, \ldots, N_j/2 - 1$ of subseries j a phase shift φ_n is randomly generated with a probability density function $\mathcal{F}_n(\varphi)$ spanned on $S_n(\varphi)$. This step introduces the necessary randomness into the encryption procedure. As a result, infinitely many phase shift encryptions φ_n are possible, i.e. infinitely many possible cyphertexts for a single cleartext subseries. Nevertheless,

the cleartext turns out to be always uniquely encryptable given the knowledge of the first and second key sequences.

Next, the generated phase shift series φ_n, $n = 1, 2, \ldots, N_j/2 - 1$ is extended by adding deterministic values of φ_0 and $\varphi_{N_j/2}$.

3. At the third stage, the extended phase shift series ϕ_n, $n = 0, 1, \ldots, N_j/2$ is considered to be the *phase spectrum* of an N_j-lag WMRTS. The amplitude spectrum of this N_j-lag WMRTS is obviously flat and equal to a. These amplitude and frequency spectra (i.e. the resulting DFT's $W^{N_j}(\Omega m)$) are transformed into the time-domain using the inverse DFT as given by any of the FFT algorithms. The resulting time-series $w^{N_j}(i)$ is a realization of an N_j-lag WMRTS. Its sine components for $n = 1, 2, \ldots, N_j/2 - 1$ have phase shifts corresponding to the characters C_n of the cleartext. Therefore it is a cyphertext for the cleartext.

   The mechanism of FFT is such that any phase shift φ_n is *dispersed* into all N_j samples of the N_j-lag WMRTS according to the one-to-one mapping

$$\left[a, \varphi(0), \varphi(1), \ldots, \varphi(N_j/2)\right] \rightarrow \left[w^{N_j}(0), w^{N_j}(1), \ldots, w^{N_j}(N_j - 1)\right] \quad (16)$$

   This means that the proposed method encrypts any character of the cleartext into all samples of the N_j-lag WMRTS cyphertext. This has a profound implication for the robustness of the encryption method: any attempts at breaking any part of the N_j-lag WMRTS cyphertext are doomed to failure for the simple reason that being *fragments* they do not contain *full information* about any character of the cleartext. This property is at the root of the robustness of the method towards breaking. This property is also at the root of the robustness of the method with respect to random disturbances which might influence the values of some of the N_j-lag WMRTS samples.

4. To improve things further (i.e. to make the encryption virtually *genius-proof*), the N_j-sample N_j-lag WMRTS $w(i)$ may be looked upon as representing some of the phase shifts used to generate a *quadruply enhanced* * $4N_j$-sample $4N_j$-lag WMRTS by the same process, and so on.

It should be noticed that:

- The proposed approach is essentially an *enhancement* of the primary series of random phase shifts ϕ_n. The N_j-lag WMRTS $w(i)$ turns out to be of much better quality (i.e. *more random*) than this primary series: this is due to the *randomization effect* achieved by choosing a *flat-spectred* frequency-domain representation $W^N(\Omega m)$, which forces *white-noise quality* into the cyphertext. This quality is particularly striking for short series.

* The fact that a *double enhancement* cannot be accomplished is due to the constraint on the phase shift for the middle-of-the-range frequency, i.e. $\phi_{N_j/2} = \pi/2$ for an N_j-lag WMRTS.

- The phase shift series ϕ_n is invariant to the change of the amplitude a.
- The knowledge of the amplitude a is not necessary to decrypt the cleartext.
- Each line of the spectrum $W^N(j\Omega m)$, being a complex number, carries information about one particular phase shift ϕ_n. However, the value of any phase shift ϕ_n gets dispersed on *all* N_j samples of the N_j-lag WMRTS $w(i)$, which contributes heavily to the power and impregnability of the method.
- In order to increase the noise robustness of the method, it is desirable to start the encryption using the highest-frequency sines first, then the next highest, and so on, leaving the lowest-frequency sines eventually unused at all. The fact that noise robustness is better the higher the frequencies of the sines used for embedding characters, is intuitively obvious: high-frequency sines give, for a given N_j, more periods for computing the phase shifts than low-frequency sines.
- The opportunity to use exclusively high-frequency sines for data encryption appears quite naturally when *quadruply enhancing* the first-generation N_j-lag WMRTS because of the abundance of frequencies which may be used to encrypt data.

5. Decrypting the N-Lag WMRTS Cyphertext

Decryption of the N-lag WMRTS cyphertext is performed in the following steps:

1. The cyphertext is partitioned into time-series of length N_j, $j = 1, 2, \ldots, k$. These time-series are of course N_j-lag WMRTS's.
2. The N_j-sample DFT is computed for the N_j-lag WMRTS using some FFT algorithm. This amounts to using the one-to-one mapping (16) in the opposite direction. As a result, the complete phase spectrum φ_n, $n = 0, 1, \ldots, N_j/2$ is obtained. The phases $\varphi(0)$ and $\varphi(N_j/2)$ are removed.
3. For the remaining phase shifts φ_n, $n = 1, 2, \ldots, N_j/2$ the intervals $S_n(\varphi)$ are determined using the *one-to-one* mapping $\varphi \to S_m(\varphi)$.
4. For the intervals $S_n(\varphi)$ the characters are determined from the one-to-one mapping $C_n \to S_n(\varphi)$.

6. An Example

Consecutive phase-shift subintervals of width $2\pi/26$ each were assigned to all 26 capital letters of the latin alphabet. Moreover, a uniform probability density function was assigned to each phase shift subinterval. This means that the phase shift for letter A was generated randomly from the subinterval $2\pi/26 \pm 2\pi/52$, for letter B—from the subinterval $4\pi/26 \pm 2\pi/52$ and so on.

Consider the following famous lines, delivered by Mackbeth to Seyton, on hearing of the death of the Queen:

> Out, out brief candle! Life's but a walking shadow; a poor player,
> That struts and frets his hour upon the stage,
> And then is heard no more; it is a tale
> Told by an idiot, full of sound and fury,
> Signifying nothing.

For any letter appearing in this cleartext, a random phase shift was generated from the subinterval probability density function corresponding to this letter. The result is shown in Table 1.

The diagram of the phase-shift series ($\phi(n)$ for $n = 1, 2, \ldots, 164$) from Table 1, shown in Fig. 1, may be regarded as an intermediate stage in the process of encryption. It is presented in order to illustrate the *enhancement of randomness* eventually achieved for the cyphertext as compared with the randomness of the phase-shift series. For that purpose, the normalized unbiased autocorrelation function estimate of the phase shifts $\phi(n)$ with removed mean value is presented in Fig. 2. Obviously, its *whiteness* leaves much to be desired.

Now, N is chosen as equal to 512. The final 512-lag WMRTS denoted by $w^{512}(i)$ and generated in such a way that the 165 phase shifts for high frequencies (i.e. φ_n for $n = 91, 92, \ldots, 255$) are used for embedding letters while low-frequency phase shifts $\phi(n)$ for $n = 1, 2, \ldots, 255 - 165$ are chosen as random and evenly distributed in the range $[0, 2\pi)$ is shown in Fig. 3.

The normalized unbiased autocorrelation function for the 512-lag WMRTS is presented in Fig. 4. The enhancement of whiteness is obvious. However, to make the argument more solid, an autoregressive model was fitted to the time-series from Fig. 4 using the AIC criterion (Söderström and Stoica, 1988). As a result, the following first-order model was obtained:

$$w^{512}(i) = \frac{1.046}{1.000 - 0.001z^{-1}} e(i)$$

$e(i)$ being the hypothetical white noise excitation with variance 1 and z^{-1} being the unit-delay operator. The smallness of the coefficient of z^{-1} clearly shows that $w^{512}(i)$ may indeed be regarded as white noise.

All simulations were performed using the *EFPI (Expert for Process Identification)* package (Niederliński *et al.*, 1991).

Both the autocorrelation function from Fig. 4 and the result of fitting the autoregressive model clearly demonstrate that the encrypted text is indeed *full of sound and fury* and seems to *signify nothing*.

7. Themes and Variations

The N-lag WMRTS produced in the previous example may arouse a suspicion in professional code breakers by being *too good to be true*. The proposed approach opens a wide range of *themes and variations* for generating less suspicious time-series.

Table 1. Random phase shifts generated for consecutive letters of the cleartext.

Char	n	$\phi(n)$	*Char*	n	$\phi(n)$	*Char*	n	$\phi(n)$	*Char*	n	$\phi(n)$
O	1	3.68533	P	45	3.87781	A	88	0.33508	F	130	1.47320
U	2	5.13909	L	46	2.96151	N	89	3.38853	U	131	5.12357
T	3	4.87685	A	47	0.27483	D	90	1.02232	L	132	2.99885
O	4	3.70980	Y	48	6.05972	T	91	4.91470	L	133	3.01818
U	5	5.16827	E	49	1.24098	H	92	2.01268	O	134	3.72115
T	6	4.85396	R	50	4.37505	E	93	1.30111	F	135	1.48220
B	7	0.58224	T	51	4.84017	N	94	3.46511	S	136	4.62062
R	8	4.42987	H	52	2.01860	I	95	2.18423	O	137	3.63119
I	9	2.28034	A	53	0.26354	S	96	4.71217	U	138	5.10190
E	10	1.32015	T	54	4.84444	H	97	2.02816	N	139	3.49341
F	11	1.52029	S	55	4.64659	E	98	1.28756	D	140	0.97172
C	12	0.84276	T	56	4.85063	A	99	0.25492	A	141	0.25324
A	13	0.31060	R	57	4.41012	R	100	4.37886	N	142	3.42923
N	14	3.42444	U	58	5.16475	D	101	0.99641	D	143	0.98705
D	15	1.03427	T	59	4.85451	N	102	3.45337	F	144	1.52397
L	16	2.99578	S	60	4.68770	O	103	3.69455	U	145	5.19229
E	17	1.25872	A	61	0.31245	M	104	3.20923	R	146	4.45909
L	18	3.00480	N	62	3.41615	O	105	3.69820	Y	147	6.11580
I	19	2.20814	D	63	1.08690	R	106	4.38561	S	148	4.65849
F	20	1.55001	F	64	1.49609	E	107	1.24526	I	149	2.18082
E	21	1.23219	R	65	4.35110	I	108	2.28147	G	150	1.71258
S	22	4.63315	E	66	1.21716	T	109	4.84676	N	151	3.45342
B	23	0.50966	T	67	4.88798	I	110	2.28815	I	152	2.22591
U	24	5.17235	S	68	4.61389	S	111	4.62066	F	153	1.49090
T	25	4.91329	H	69	2.03463	A	112	0.36176	Y	154	6.06344
A	26	0.34189	I	70	2.23628	T	113	4.93487	I	155	2.22655
W	27	5.67492	S	71	4.61637	A	114	0.28019	N	156	3.47717
A	28	0.33188	H	72	1.99237	L	115	2.93824	G	157	1.71590
L	29	2.93928	O	73	3.65802	E	116	1.28580	N	158	3.41158
K	30	2.75240	U	74	5.10504	T	117	4.90493	O	159	3.74574
I	31	2.29358	R	75	4.43420	O	118	3.69344	T	160	4.85301
N	32	3.46169	U	76	5.15265	L	119	2.96763	H	161	2.01282
G	33	1.73686	P	77	3.91656	D	120	1.05049	I	162	2.26316
S	34	4.68669	O	78	3.65925	B	121	0.50422	N	163	3.43720
H	35	1.96625	N	79	3.39404	Y	122	6.12942	G	164	1.79614
A	36	0.29923	T	80	4.87729	A	123	0.25016			
D	37	1.08657	H	81	1.95617	N	124	3.47441			
O	38	3.67178	E	82	1.30349	I	125	2.27958			
W	39	5.59774	S	83	4.66329	D	126	1.00737			
A	40	0.30453	T	84	4.84880	I	127	2.27338			
P	41	3.94404	A	85	0.33591	O	128	3.72337			
O	42	3.70266	G	86	1.73721	T	129	4.85212			
O	43	3.62501	E	87	1.28820						
R	44	4.41293									

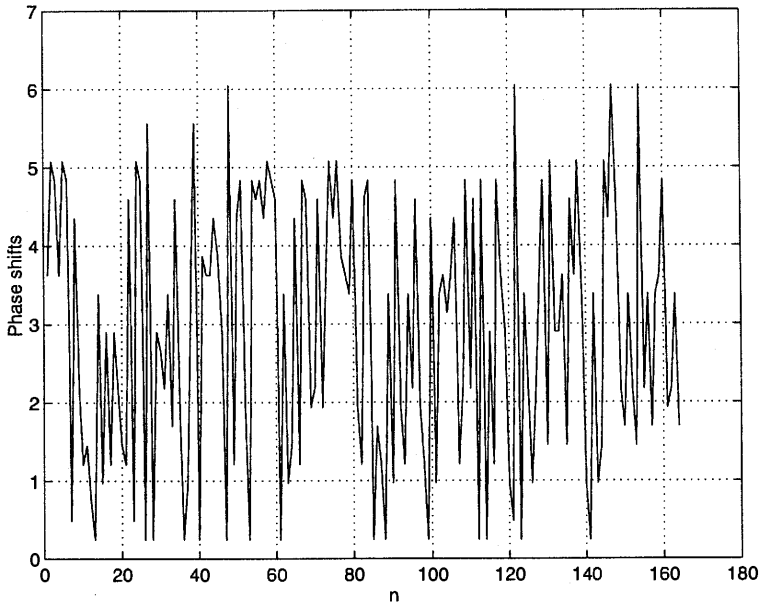

Fig. 1. The diagram of the phase-shifts encrypted cleartext from Table 1.

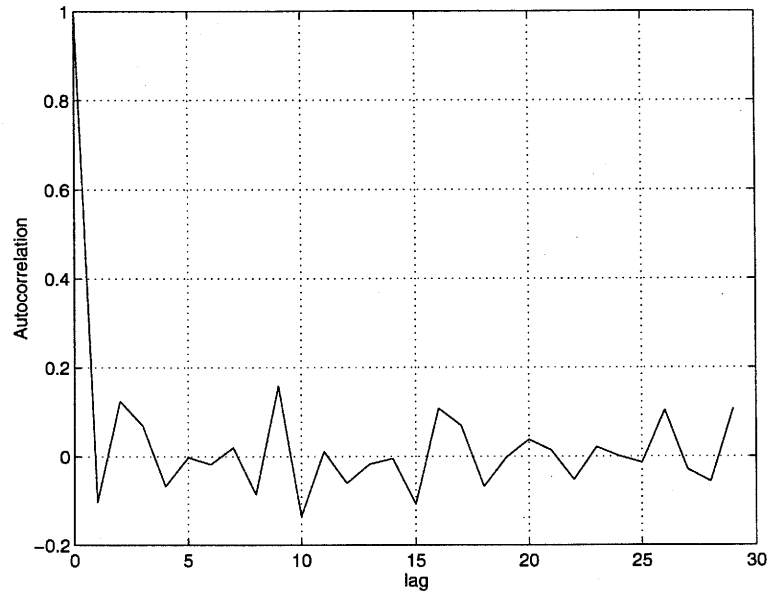

Fig. 2. The normalized unbiased autocorrelation function for the phase shift series of Fig. 1 with removed mean value.

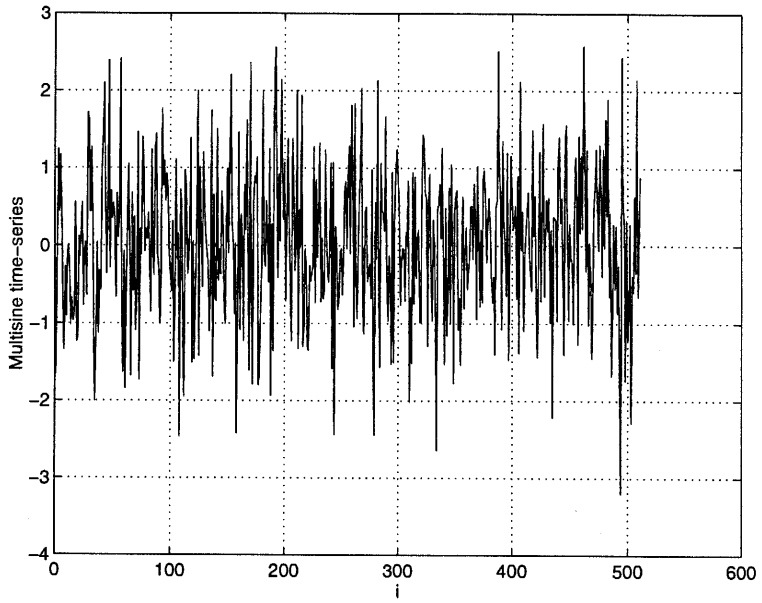

Fig. 3. The 512-lag white multisine time-series generated from the phase shift of Fig. 1.

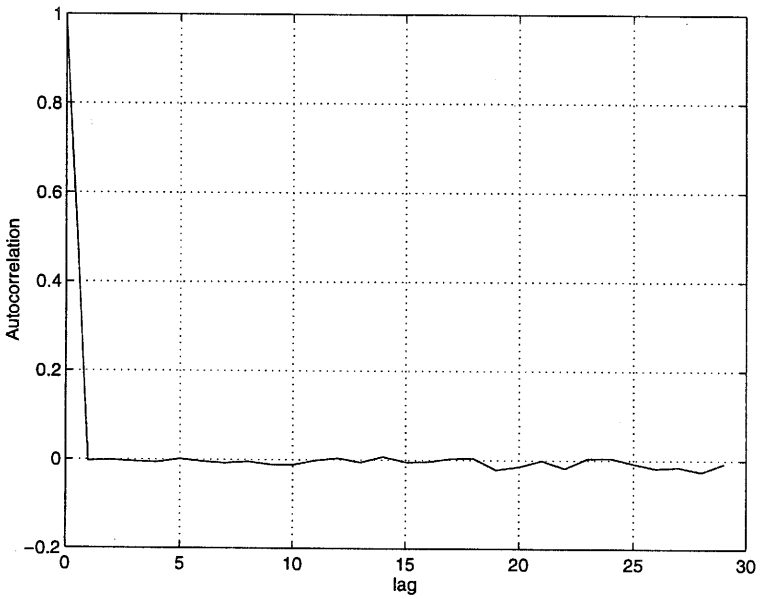

Fig. 4. The normalized unbiased autocorrelation function for the 512-lag white multisine time-series of Fig. 3.

The most obvious variation is to relax the condition of equal amplitudes while retaining the basic idea of using phase shifts to represent data characters. A particular interesting possibility is to choose the A_n amplitudes as random and evenly distributed in some range (AMAX,AMIN) and to encrypt the cleartext using relations corresponding to those presented in Section 4 followed by the FFT. It should be remembered that the knowledge of the A_n amplitudes is not necessary to get (*via* the FFT) the DFT from the cyphertext $u^N(i)$ and to determine from it the phase shifts ϕ_n, so no additional key sequences are necessary and the only (small) additional trouble is with taking into account the nontrivial amplitude spectrum while generating the DFT. The additional havoc created in the cyphertext by sines having random amplitudes may be more than worthwhile this small trouble.

The next variation is to use as the trapdoor predicate (Goldwasser and Micali, 1984) a filter for which:

- it is easy to compute an output for a given N-lag WMRTS input but
- it is difficult to identify filter parameters in order to calculate the N-lag WMRTS input on the basis of the knowledge of the output without additional trapdoor information.

This trapdoor information may be a part of the key sequence.

8. Conclusions

This paper has argued for a new approach to data encryption: it is proposed to put the cleartext directly into the phase shifts of the DFT-representation of an N-lag white multisine random time-series, which in turn is synthesized from this DFT representation using any of the powerful FFT algorithms. The advantages of the proposed method are as follows: (1) For any cleartext there are infinitely many possible cyphertexts which may be uniquely decoded using two simple *key sequences*. (2) Each character of the cleartext contributes to all samples of the time-series, no matter how large is the number of samples. (3) By using any of the powerful FFT algorithms, it is possible to swiftly encrypt a cleartext and to decrypt a cyphertext of any length. (4) The cleartext characters being encoded as phase shift intervals, the proposed method is robust with respect to cyphertext amplitude changes and additive noise.

The basic mechanism of the method may be *nested* by considering the N-lag white multisine random time-series as representing phase shifts for a $4N$-lag white multisine random time-series, and so on.

The method may be modified by retaining the basic principle of using phase shifts to represent data.

Silicon implementations of FFT algorithms in various signal processors make encrypting and decrypting time-series of any length particularly attractive.

Acknowledgement

The partial financial support of this research by the Polish State Committee for Scientific Research (KBN) under project BK-201/RAu-1/98 is gratefully acknowledged.

References

Bendat J.S. and Piersol A.G. (1986): *Random Data Analysis and Measurement Procedures.* — New York: Wiley.

Denning D. (1983): *Cryptography and Data Security.* — New York: Addison-Wesley.

DES (1977): *Data encryption standard*, In: Federal Information Processing Standards Publication. — National Bureau of Standards, Washington, p.46.

Figwer J. (1997): *A new method of random time-series simulation.* — Simul. Pract. Th., Vol.5, No.3, pp.217–234.

Figwer J. and Niederliński A. (1992): *On the generation of high quality scalar white noise series.* — Appl. Stoch. Mod. Data Anal., Vol.8, No.4, pp.311–326.

Figwer J. and Niederliński A. (1995): *Using the DFT to synthesize multivariate orthogonal white noise series.* — Trans. Soc. Comp. Simul., Vol.12, No.4, pp.261–285.

Figwer J., Niederliński A. and Kasprzyk J. (1993): *A new approach to the identification of linear discrete-time MISO systems.* — Arch. Contr. Sci., Vol.2 (XXXVIII), No.3–4, pp.223–239.

Goldwasser S. and Micali S. (1984): *Probabilistic encryption.* — J. Comp. Syst. Sci., Vol.28, pp.270–279.

Koblitz N. (1994): *A Course in Number Theory and Cryptography.* — New York: Springer-Verlag.

Niederliński A. and Figwer J. (1995): *Using the DTF to synthesize bivariate orthogonal white noise series.* — IEEE Trans. Sign. Process., Vol.43, No.3, pp.749–758.

Niederliński A., Figwer J. and Kasprzyk J. (1991): *EFPI—An integrated intelligent software environment for system and signal identification.* — Prep. 9th IFAC/IFORS Symp. *System Identification and Parameter Estimation*, Vol.1, Budapest, Hungary, pp.567–572.

Nussbaumer H.J. (1982): *Fast Fourier Transform and Convolution Algorithms.* — New York: Springer.

Oppenheim A.V. and Schafer R.W. (1975): *Digital Signal Processing.* — Englewood Cliffs: Prentice Hall.

Schneider B. (1994): *Applied Cryptography, Protocols, Algorithms and Source Code in C.* — New York: Wiley.

Söderström T. and Stoica P. (1988): *System Identification.* — Hemel Hempstead: Prentice-Hall.

Received: 23 June 1997
Revised: 3 February 1998