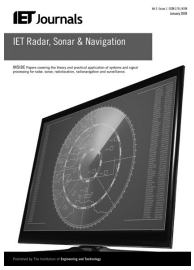
Published in IET Radar, Sonar and Navigation
Received on 4th February 2014
Revised on 25th June 2014
Accepted on 10th July 2014
doi: 10.1049/iet-rsn.2014.0066



ISSN 1751-8784

Pulse compression security enhancement as an electronic protection technique by exploiting a block cipher output as phase-code

Nader Sanandaji, Mohammad Soleimani

Department of Electrical Engineering (Antenna and Microwave Lab), Iran University of Science and Technology (IUST), Tehran, Iran
E-mail: Sanandaji@elec.iust.ac.ir

Abstract: In this study, the exploitation of a block cipher output as phase-code for pulse compression in a radar system is introduced. This method is as an effective electronic protection technique against some electronic intelligence-based electronic attacks. Security enhancement of the mentioned scheme is discussed and some autocorrelation properties of it are investigated. Probabilities of false alarm and detection in case of using a block cipher generated phase-code are also studied. A new method for countering the effects of repeater jammers and digital radio frequency memories is also proposed which is based on block cipher encryption key update. This new method tries to implement a low probability of identification radar. All of the mentioned subjects are investigated by mathematical equations and simulation verifications.

1 Introduction

Since radar systems have been introduced, there have been lots of efforts to degrade or neutralise their effectiveness by means of different measures. These measures are categorised as a class of 'electronic attack' (EA) which is a division of 'electronic warfare' (EW) [1]. One of the main executives of EA is jamming. Jammers transmit high-power signals to deceit radars by creating false targets or masking real targets [2, 3].

On the other hand, through 'electronic support' (ES), current EA systems, exploit 'electronic intelligence' (ELINT) to intercept radar's signals and analyse them [2]. Through developments in digital signal processing and storage in recent years, digital 'radio frequency memory' (DRFM) structures are widely used in EW to intercept, analyse, identify and retransmit the intercepted signals of radars. DRFMs are employed by 'repeater' jammers which retransmit signals similar to radar's and deceit the radar by creating ghosts in unreal range gates or velocity gates [4, 5].

The efforts to counter the effects of EA are classified as a type of electronic protection (EP). One of the most practical levels for implementing EP against EA, is the radar receiver corresponding to a specific transmitter and waveform. The main method in this level is to use pulse compression [6]. In this technique, improved range resolution and signal-to-noise ratio (SNR) are achieved by spreading the spectrum of radar's transmitted signal and using a proper filter (usually a matched filter) in radar receiver [7]. Digital pulse compression is done by employing phase-codes and frequency codes. Digital phase-coded waveforms that are the subject of this article can provide an acceptable persistence against interception and also jamming [7, 8]. However, it should be mentioned that 'coded' jammers can still pose serious threats on radar receiver performance even if a phase-coded waveform is used in a radar system [9]. A code which is used to modulate the phase of a radar waveform must be completely confidential and the ELINT of the ES unit should have no access to or predict any part of it. If the phase-code be disclosed, then the interceptor of ES unit can set its receiver filter coefficients in a manner that will be able to compress the received signal to intercept it successfully. The other threat of phase-code disclosure is the fact that the coded jammer of an EA unit can modulate its jamming signal in a manner that the interfering signal be compressed successfully in radar receiver to increase the false alarm rate [10, 11]. The mentioned threats accentuate the importance of phase-code confidentiality and security. On the other hand, according to one of the main encryption principles known as 'Kerckhoff's' assumption, confidentiality and security of a code must be imposed in the key used to generate the code rather than the generating algorithm. This assumption is based on the worst-state scenario in which the adversary, finds the algorithm employed in radar's pulse compression code generator through various manners (such as cryptanalysis and ELINT methods by interception or physical access in an EW and battlefield situation). The Kerckhoff's assumption states that if the cryptographic terms are applied in code generation, the adversary cannot predict any part of the code by just having algorithm and not confidential key used to generate the code [12]. Therefore in case of an EW scenario, any phase-code used in pulse compression should be generated using a secure and confidential key-based algorithm [13].

In addition to security, the phase-code must have proper features related to its autocorrelation. In other words, the output of radar receiver filter (matched or mismatched) must have low sidelobes compared with the mainlobe. Two main criteria to measure this feature are 'integrated sidelobe ratio' (ISR) and 'peak sidelobe ratio' (PSR). Hence, each code used in pulse compression must be evaluated in terms of ISR and PSR.

In this article, we propose exploiting an ideal block cipher output as a confidential phase-code for bi-phase pulse compression. This is a key-based method and therefore can be a perfect candidate for application in EW. By investigating PSR, ISR and comparing them with M-sequences' autocorrelation properties, we prove that these confidential key-based codes can be good choices to be employed in pulse compression as an EP.

2 Security and confidentiality of a phase-code generated by block cipher

ELINTs play a key role in modern EW systems which should be considered in the design of any phase-coded waveforms for EP. Before the evolution of ELINT systems, sequences such as Barker codes or maximal length codes were largely used for pulse compression in radar. Since there are only a few number of known Barker codes, an ES unit can predict the employed Baker code easily. On the other hand, M-sequences are also vulnerable to some cryptanalysis. A well-known security deficiency of these codes is that if the length of M-sequence be N, where $N = 2^r - 1$, then the ES unit interceptor can predict the whole code by intercepting $2r$ consecutive bits of the code [14]. Many approaches have been introduced for generating phase-codes for pulse compression such as conjunctions of different 'linear feedback shift registers' or using non-linear feedback shift registers to improve the security level of pulse compression [15]. However, the security of these approaches depends on the algorithm used to generate the phase-code and the generated code may be vulnerable to different cryptanalysis techniques used in ELINT systems. According to well-known pseudorandom and confidential code generation principles, a confidential code must have all of the following features [16]:

- The code should prove itself as random in some well-known randomness tests.
- The cryptanalysis without any information about the encryption key, even in condition of access to many bits, should not be able to predict the forthcoming bits.
- Values of all bits in the code should be independent from each other.

The mentioned features imply the complexity of a phase-code generation. Here in this article, we propose the use of a block cipher as a phase-code generator for pulse compression which can satisfy all mentioned features [16].

3 Peak sidelobe ratio and integrated sidelobe ratio of a phase-code generated by block cipher

If the radar receiver filter be matched to the transmitted waveform replica which is assumed to be a complex signal denoted by $s_i(t)$, then, in condition of no interference except additive white Gaussian noise (AWGN), the output of this filter because of an echo of a target can be written as

$$y(t) = Cs_o(t-d) + n_o(t) \tag{1}$$

where C is a parameter related to radar range equation, $s_o(t)$ is the output because of a target echo, d is the delay time related to distance of target from radar antenna and $n_o(t)$ is the component caused by the AWGN at the output of the matched filter. If we denote the impulse response of matched filter by $h(t)$, then for normalised component of signal at matched filter output we have

$$s_o(t) = \frac{1}{\tau} s_i(t) * h(t) \tag{2}$$

where '*' denotes convolution and τ is the pulse width. Because we used matched filter in receiver, $h(t)$ is the same as complex conjugate time-reversed of $s_i(t)$. Hence we can rewrite (2) as

$$s_o(t) = \frac{1}{\tau}\int_0^{\tau} s_i(u) s_i^*(\tau - t + u)\, \mathrm{d}u \tag{3}$$

In the above equation, τ is the duration of radar pulse modulated by confidential block cipher generated phase-code and $s_i^*(\tau - t)$ is the conjugated time-reversed version of $s_i(t)$. Considering the value of pulse compression gain to be N, then the duration of each sub-pulse would be τ' which equals to τ/N. Thus for $s_i(t)$ we can write

$$s_i(t) = \sum_{n=0}^{N-1} a_n P(t - n\tau') \tag{4}$$

In which, $P(t)$ is a pulse of power p_s beginning at 0 and ending at τ' and a_n is the nth bit of the phase-code generated by block cipher after mapping 0 values to -1 and 1 to +1. Considering $t = k\tau' + \tau_{\in}$, where $0 \le \tau_{\in} < \tau'$, then by substituting (4) in (3) and some mathematical manipulations it can be proven that (3) would be [10]

$$s_o(t) = \left(1 - \frac{\tau_{\in}}{\tau'}\right)\theta_a(k) + \frac{\tau_{\in}}{\tau'}\,\theta_a(k+1) \tag{5}$$

where $\theta_a(k)$ is the 'discrete autocorrelation function' of waveform which is defined here as

$$\theta_a(k) = \frac{p_s}{N}\sum_{n=0}^{N-1} a_n a_{n-k}^*, \quad 0 < n < N-1 \tag{6}$$

Since $\tau_{\in}/\tau'$ is considered to be very small in (5), thus an acceptable estimate for the value of radar receiver matched filter output is the discrete autocorrelation function denoted by $\theta_a(k)$ in (6) and this value can represent the autocorrelation properties of waveform used in radar [6, 10].

If we consider unpredictability of a block cipher output as one of its main security points, then it means that the value of a_n terms for $0 < n < N$, are independent and accept -1 and +1 with same probabilities equal to 1/2. Hence, we can say that $a_n a_{n-k}$ for $k \neq 0$ is a discrete random variable with the

doi: 10.1049/iet-rsn.2014.0066

following 'probability density function' (PDF)

$$\begin{aligned} &P[a_n a_{n-k}=1]=P[a_n=1]P[a_{n-k}=1] \\ &+P[a_n=-1]P[a_{n-k}=-1]=\frac{1}{4}+\frac{1}{4}=\frac{1}{2} \\ &P[a_n a_{n-k}=-1]=P[a_n=-1]P[a_{n-k}=1] \\ &+P[a_n=1]P[a_{n-k}=-1]=\frac{1}{4}+\frac{1}{4}=\frac{1}{2} \end{aligned} \tag{7}$$

Equation (6), is in fact the summation of 'N independent and identically distributed' (iid) random variables of $a_n a_{n-k}$. Now, if the pulse compression gain or N be a large value (which is over 30 dB in most radar applications), then according to central limit theorem, the value of $\theta_a(k)$ is a Gaussian random variable. By normalising the power of transmitted pulse and assuming that p_s is unit (this assumption makes no change in universality of investigation), for each $k \neq 0$, the PDF of discrete autocorrelation function would be

$$f_{\theta_a}[\theta_a(k)]=\frac{1}{\sqrt{2\pi/N}}\mathrm{e}^{-([\theta_a(k)]^2 N)/2} \tag{8}$$

The value of ISR is defined as

$$\mathrm{ISR}=\frac{2\sum_{k=1}^{N-1}|\theta_a(k)|^2}{N^2} \tag{9}$$

By substituting $\theta_a(k)$ in (9), the value of ISR will become a random variable. The square of a Gaussian variable is a Chi-square variable with one degree of freedom. Hence the PDF of random variable $|\theta_a(k)|^2$ would be

$$|\theta_a(k)|^2 \sim \chi^2(1) \tag{10}$$

And for mean and variance of this random variable, we have

$$\begin{aligned} E\{|\theta_a(k)|^2\}&=\sigma^2_{\theta_a(k)}+E\{\theta_a(k)\}^2,\ \sigma^2_{|\theta_a(k)|^2} \\ &=2\sigma^2_{\theta_a(k)}\left(\sigma^2_{\theta_a(k)}+2E\{\theta_a(k)\}^4\right) \end{aligned} \tag{11}$$

Thus, the expected value and variance of this random variable is

$$E\{|\theta_a(k)|^2\}=\frac{1}{N},\ \sigma^2_{|\theta_a(k)|^2}=2\frac{1}{N}\left(\frac{1}{N}+0\right)=\frac{2}{N^2} \tag{12}$$

And since all $|\theta_a(k)|^2$ random variables are iid, and N was assumed to be a large number, according to central limit theorem, the random variable ISR would have a Gaussian PDF with the following mean and variance

$$E\{\mathrm{ISR}\}=\frac{2(N-1)}{N^3},\quad \sigma^2_{\mathrm{ISR}}=\frac{8(N-1)}{N^6} \tag{13}$$

The expected value of ISR can be a good estimate of this important criterion thus according to (13), for large values of N, we have

$$\lim_{N\to\infty}\frac{2(N-1)}{N^3}\equiv\lim_{N\to\infty}\frac{2}{N^2} \tag{14}$$

To compare the value of ISR in case of using an M-sequence as phase-code, which its autocorrelation properties are considered to be much better than many other phase-codes, its discrete autocorrelation function must be investigated first. According to well-known spread spectrum references, discrete autocorrelation function of M-sequence codes can be written as [10]

$$\theta_a(k)=\begin{cases}1 & k=mN\\ \dfrac{-1}{N} & k\neq mN\end{cases} \tag{15}$$

where in equation above, N is the period of the M-sequence and m is an integer. By substituting (15) in (9), the value of ISR for an M-sequence would be

$$\mathrm{ISR}_{M\text{-seq}}=\frac{2(N-1)}{N^4} \tag{16}$$

For a large value of N, as in many radar systems this value is larger than 30 or 40 dB, we have

$$\lim_{N\to\infty}\frac{2(N-1)}{N^4}=\lim_{N\to\infty}\frac{2}{N^3} \tag{17}$$

It can be concluded by comparing (14) and (17) that the ISR of a block cipher generated phase-code has inverse relation with the square of the pulse compression gain, while for an M-sequence it has inverse relation with the cube of the pulse compression gain. Although this difference is tangible, but in practice, the value of thermal noise or other interferences such as clutter, completely masks and overshadows this difference.

The result of computer simulation for a pulse compression gain of 500 for a block cipher generated phase-code and an M-sequence with period 255 chips is demonstrated in Fig. 1 for 31 range gates (normalised delays matched on 0–30 range gate). The result of simulation has many more

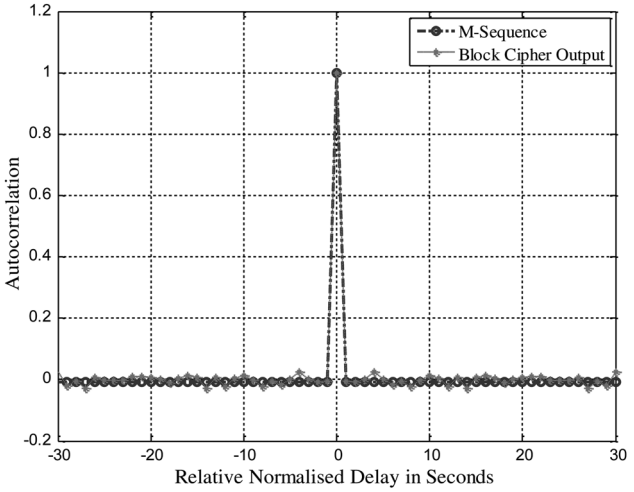


Fig. 1 *Comparison of autocorrelation of an M-sequence with period 255 with a block cipher output code with length 500*

normalised delays but in order to have a clear illustration, only 31 time delays are plotted.

The PSR is defined as the ratio of the maximum value of sidelobes at the output of the matched filter to the value of mainlobe. Since the power of the pulse transmitted by radar is considered to be normal, the value of mainlobe equals to one. Based on (8), PSR of a block cipher generated phase-code is a random variable. The value of the PSR is also a random variable which equals to the maximum of a Gaussian vector with N components each with PDFs as (8). Since the calculation of this PDF is complicated therefore we used computer simulation for some values of N. Simulation results can be summarised as follows.

For pulse compression gain in range of 20–30 dB, the PSR would be in range of −10 to −15 dB and for large values of pulse compression gain more than 40 dB, the PSR would be lower than −25 dB which means signal to sidelobe ratio in worst-case (inverse of the PSR) is less than 25 dB. In practice, this PSR is far less than signal to thermal noise ratio or signal to clutter ratio which implies the fact that in the case of employing an appropriate pulse compression gain (more than 30 dB), sidelobes are less effective than other interferences such as noise and clutter.

If we compare the value of the PSR in the case of using block cipher output as phase-code with the condition of employing an M-sequence, it is implied that the PSR properties of a block cipher output as phase-code are definitely inferior to M-sequences or any other well-known phase-codes such as Barker codes. Considering the use of an M-sequence code with period N, then the value of the PSR would be $1/N$ which means for a pulse compression gain of 30 dB it has a PSR of −30 dB, while simulation results for the condition of employing a block cipher output as phase-code for a pulse compression of gain 30 dB, will result in a PSR of about −15 dB which shows a significant difference with M-sequences. Thus it could be said that losing a desirable value of PSR is the main cost of achieving a higher level of security. However, security is usually of much higher priority in EW situations.

4 Probability of false alarm in the case of using block cipher generated phase-codes

In this section, the probabilities of false alarm and detection are investigated. By employing a block cipher output as phase-code, and also considering the output of the matched filter as (1), then the values of discrete autocorrelation function for each normalised delay denoted by $k \neq 0$ in (6) to (8) correspond to sidelobes of each range gate and the value of discrete autocorrelation function for $k = 0$ corresponds to the mainlobe. The values of sidelobes at $k \neq 0$ are considered as unfavourable interferences causing false alarm. On the other hand, according to (8), $\theta_a(k)$ can be considered a discrete Gaussian random process for every $k \neq 0$ and all components of this process are independent because of the independence of block cipher output bits. If the block cipher algorithm designed to generate a phase-code of length N be ideal, then all random variables of a_n for $0 < n < N$–1 would be independent. Thus by referring to (8), the values of discrete autocorrelation function's samples denoted by $\theta_a(k)$ for every $k \neq 0$ would be independent from each other. It can be easily proved that this random process is also a wide-sense stationary one and therefore it can be considered as a Gaussian noise process. According to Wiener–Khinchin theorem, we can say the variance of components corresponds to the value of the Gaussian variables' variance. Hence as shown in (8), it can be assumed that if the pulse compression gain denoted by N be a large value, then the matched filter output sidelobes' properties resemble a Gaussian variable with zero mean and variance of p_s/N.

Now if we write the in-phase and quadrature components of matched filter output for $k \neq 0$, we have

$$\begin{aligned} v_I(k) &= \theta_{a,I}(k) + n_I(k) \\ v_Q(k) &= \theta_{a,Q}(k) + n_Q(k) \end{aligned} \tag{18}$$

where $\theta_{a,I}(k)$ and $\theta_{a,Q}(k)$ are in-phase and quadrature components of sidelobe and $n_Q(k)$ and $n_I(k)$ are in-phase and quadrature components of Gaussian noise at the output of the matched filter. According to filtered Gaussian process theorems, in-phase and quadrature components of Gaussian processes like $n(k)$ and $\theta_a(k)$, are uncorrelated stationary processes with the same variance and mean [17]. It should be mentioned that the input AWGN to the matched filter will result in a Gaussian but not white process at the output of the matched filter because after filtering, it has a limited band. Thus it would be a coloured process and due the fact that the matched filter is considered to be linear time-invariant, the output process is still Gaussian. Hence, we can say that $v_I(k)$ and $v_Q(k)$ for each $k \neq 0$ are Gaussian variables with zero mean and variances as

$$\psi^2 = \eta^2 + \frac{C^2 p_s}{N} = \eta^2 + \frac{A^2}{N} \tag{19}$$

where in equation above, η^2 is the variance of Gaussian noise component at the output of the matched filter related to thermal noise, A is the amplitude of the demodulated rectangular waveform at matched filter output or in other words the amplitude of the radar signal component at the output of the matched filter and C^2, which was also mentioned in (1), can be defined here as

$$C^2 = \frac{G_t G_r \lambda^2 \sigma}{(4\pi)^3 R^4 L_s} \tag{20}$$

G_t and G_r in the equation above, are radar transmitter and receiver gains, λ is the wavelength, σ is the radar cross section of target, R is the distance between radar and target and L_s is the path loss factor.

By employing a peak detector for detection, then the value of peak can be written as

$$r(k) = \sqrt{v_I^2(k) + v_Q^2(k)} \tag{21}$$

By substituting (18) in (21), and considering (19), it can be concluded that $r(k)$ is a Rayleigh random variable with the following PDF

$$\begin{aligned} f_r(r) &= \frac{r}{\psi^2} \mathrm{e}^{-r^2/2\psi^2} \\ &= \frac{r}{\eta^2 + (A^2/N)} \mathrm{e}^{-r^2/2(\eta^2 + (A^2/N))} \end{aligned} \tag{22}$$

Denoting the threshold of detection by V_T, then the

doi: 10.1049/iet-rsn.2014.0066

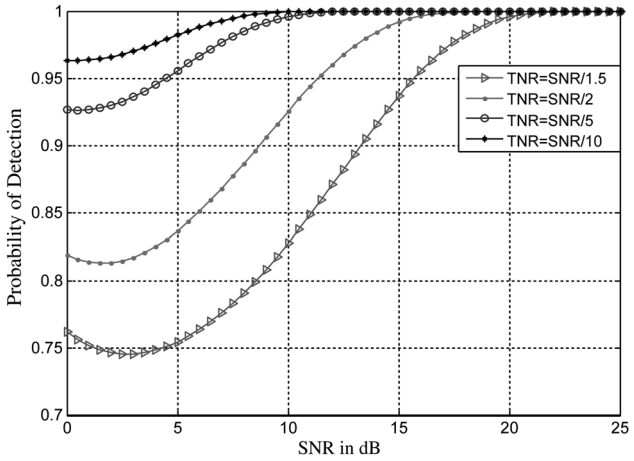


Fig. 2 *Probability of detection for four different relations between TNR and SNR in condition of using a block cipher generated phase-code with length 255 bits*

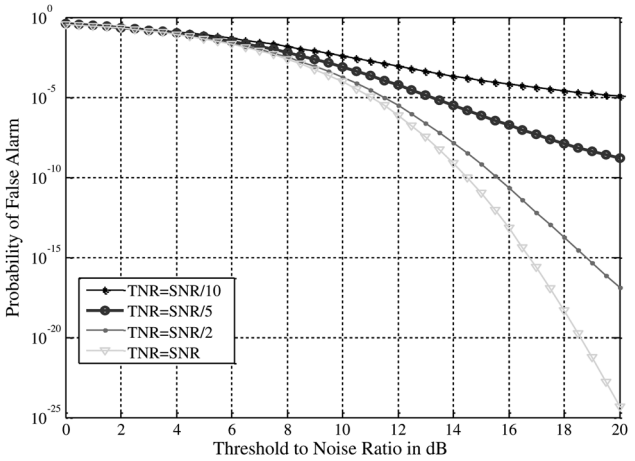


Fig. 3 *Probability of false alarm for four different relations between TNR and SNR in condition of using a block cipher generated phase-code with length 255 bits*

probability of false alarm would be

$$P_{\text{fa}} = \int_{V_T}^{\infty} f_r(r)\,\mathrm{d}r = \int_{V_T}^{\infty} \frac{r}{\eta^2 + (A^2/N)} \mathrm{e}^{-r^2/2(\eta^2+(A^2/N))}\,\mathrm{d}r = \mathrm{e}^{-V_T^2/2(\eta^2+(A^2/N))} \tag{23}$$

It should be mentioned that we have overlooked other interferences such as clutter. The probability of detection which is related to mainlobe at normalised delay of $k = 0$, always has a permanent equation in an AWGN channel regardless of the structure of phase-code and can be written as [2]

$$P_D = Q\left[\frac{A}{\eta}, \frac{V_T}{\eta}\right] \tag{24}$$

where in equation above, Q denotes the Q-Marcum function. By increasing SNR (which equals to $A^2/2\eta^2$), the probability of detection increases. However, if the detection threshold be a constant value independent of SNR, then according to (23), increasing SNR will result in a higher probability of false alarm. To avoid this deficiency, threshold of detection should be selected in accordance with the value of SNR. If we define 'threshold-to-noise ratio' (TNR) as $V_T^2/2\eta^2$, then Fig. 2, shows some simulation results for probability of detection as (24) for some relations between SNR and TNR.

It was shown that for an acceptable probability of detection in the condition of using a block cipher generated phase-code, TNR and SNR must have a specific relation. According to (23), the probability of false alarm can be rewritten as

$$P_{\text{fa}} = \mathrm{e}^{-\text{TNR}/(1+(2\text{SNR}/N))} \tag{25}$$

The simulation results for false alarm probability for some relations between TNR and SNR can be seen in Fig. 3.

5 Introducing a new method to counter repeater jammers and DRFMs effects by key update

As mentioned earlier, repeater jammers and DRFM systems exploit ELINT through their ES unit to intercept, store, identify, analyse and retransmit the signals transmitted by radars. Considering the phase-code used in pulse compression to be completely confidential, repeater jammers can still pose a significant threat on radar system. If the interceptor of an ES unit employs a filter which is not matched to radar's transmitted waveform because of phase-code confidentiality, then the output of the ES receiver filter in an AWGN channel can be written as

$$z(t) = Ks_o(t-d) + n_0(t) \tag{26}$$

In (26), $s_o(t)$ is the output component of the radar signal, $n_0(t)$ is the AWGN component at the output of the ES receiver filter, d is the delay corresponding to the distance between radar and ES unit and K is a parameter related to radar equation which is defined as

$$K = \frac{G_t G_{r_{\text{ES}}} \lambda^2}{(4\pi R)^2 L_{\text{ES}}} \tag{27}$$

where G_t is radar transmitter antenna gain, $G_{r_{\text{ES}}}$ is ES unit antenna gain in the direction of radar, λ is the wavelength, R is the distance between radar and ES unit and L_{ES} is the loss factor. In (26), $s_o(t)$ can be rewritten as

$$s_o(t) = s_i(t) * h_{\text{ES}}(t) = p_s \int_0^{\tau} P_s(t-d-u) h_{\text{ES}}(u)\,\mathrm{d}u \tag{28}$$

where $s_i(t)$ is the radar signal component at the input of the ES receiver filter, p_s is the power of the modulated pulse transmitted by radar, and $h_{\text{ES}}(t)$ is the ES receiver filter impulse response. If we denote the phase-code used for pulse compression in radar waveform by a_n and ES receiver filter phase-code by b_n, then by using the same analysis mentioned in section (3), the integral of (28) can be

represented by discrete cross-correlation of these two codes as

$$\int_0^{\tau} P_s(t-d_j-u)h_{\mathrm{ES}}(u)\,\mathrm{d}u \cong \sum_{n=0}^{N-1} a_n b_{n-k}^{*} \tag{29}$$

Since a_n is confidential, then $a_n b_{n-k}^{*}$ can be considered as a discrete random variable for all values of normalised delays denoted by k just like (7). If the pulse compression gain denoted by N be a large number, according to central limit theorem and (28), for each t, $s_o(t)$ is a Gaussian random variable as

$$f_{s_o(t)}[s_o(t)] = \frac{1}{\sqrt{2\pi N/p_s}} \mathrm{e}^{-[s_o(t)]^2 p_s/2N} \tag{30}$$

And by the same argumentation used in section (3), $s_o(t)$ is a Gaussian process which the variance of its components represents its energy spectral and equals to

$$E\left(s_o^2(t)\right) = \frac{p_s}{N} \tag{31}$$

Now, using (27) and the variance of Gaussian process in (31), the SNR at the output of ES unit would be

$$\mathrm{SNR}_{\mathrm{ES}} = \frac{p_s G_t G_{r_{\mathrm{ES}}} \lambda^2}{N(4\pi R)^2 K T_S B L_{\mathrm{ES}}} \tag{32}$$

The pulse compression gain denoted by N is a large value in most radar systems. Thus it can result in a reduced SNR at ES unit receiver which leads to a low probability of intercept radar.

Repeater jammer and DRFMs, supported by ES and ELINT, will intercept radar signals by a peak detector. Once the value of peak detector rises over a specific threshold, DRFM starts to capture the received signal. After storing the received signal in memory, the repeater jammer starts to retransmit it and a very effective jamming can reduce radar performance in a manner that even may result in a complete failure of radar function. In addition to repeater jamming, another flaw that interception may cause is that a set of stored signals of a radar system will result in the identification of radar signal. In this section, we propose encryption key update in block cipher as an EP against repeater jammers and identification of radar signals that would result in a low probability of identification radar.

If the key used in block cipher changes, then the block cipher output which is used as phase-code will be completely altered. Since it is assumed that the radar receiver filter is matched to the radar waveform replica, the repeater jammer's retransmitted signal will not de-spread or compress at the matched filter output because of the changes in the matched filter coefficients caused by the key update. The other advantage of key update is that intercepted and stored signals of radar will give no meaningful information to the adversary's ELINT because of the security features of block cipher output mentioned in Section 2.

The key update should be adjusted according to the average time that a transmitted radar signal might be intercepted or in other words the average time that the ES peak detector filter detects the radar signal. Considering (32) and (24), the

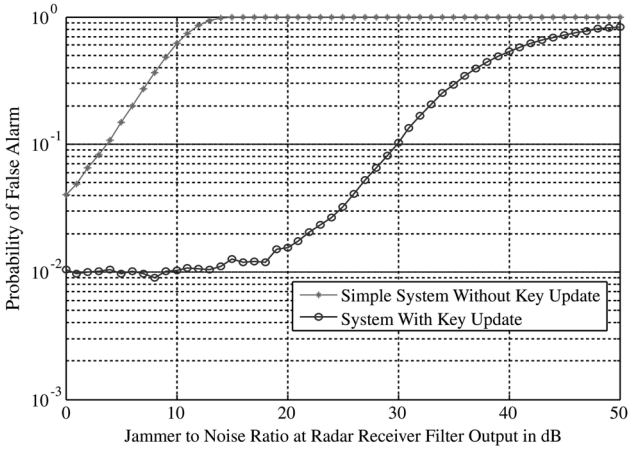


Fig. 4 *Enhancement of jamming margin against false alarm probability in case of using key update compared to a simple system without key update in the case of using pulse compression of gain 27 dB*

probability of interception (detection by ES) can be written as

$$P_{\mathrm{Intercept}} = Q\left[\sqrt{2\mathrm{SNR}_{\mathrm{ES}}},\ \frac{V_T}{\eta}\right] \tag{33}$$

Considering the ergodicity of all random processes and signals, the probability of interception can be defined as the ratio of the time when peak detector output is over the threshold to the average time that successful interception occurs. Thus we have

$$P_{\mathrm{Intercept}} = \frac{t_{\mathrm{int}}}{T_{\mathrm{Intercept}}} = \frac{\tau}{T_{\mathrm{Intercept}}} = \frac{\tau}{T_{\mathrm{Key\text{-}Update}}} \tag{34}$$

In the equation above, t_{int} is the total time when ES peak detector output is over threshold that can be estimated by radar pulse width denoted by τ and $T_{\mathrm{Intercept}}$ is the average time that a successful detection occurs which is consistent on the key update time denoted by $T_{\mathrm{Key\text{-}Update}}$.

Simulation results in Fig. 4 confirm the enhancement of endurance against repeater jammers. This figure implies that a radar receiver with key update, has a better jamming margin because at the same jammer to noise ratio, false alarm probability caused by repeater jammer for a system with key update is much lower than a system without key update.

6 Radar signal performance and ambiguity function of the phase-coded waveform by block cipher output

In this section range resolution, maximum unambiguous range and also the periodic ambiguity function in the case of employing a block cipher output as phase-code in pulse compression are discussed.

Considering pulse compression gain as N, a radar pulse of duration τ will be divided to N sub-pulses each with duration of τ' for every range gate. Now if the range resolution is matched to the length of each range gate, by denoting the light velocity by c, for range resolution we have

$$\text{Range resolution} = \Delta R = \frac{c\tau'}{2} = \frac{c\tau}{2N} \tag{35}$$

doi: 10.1049/iet-rsn.2014.0066

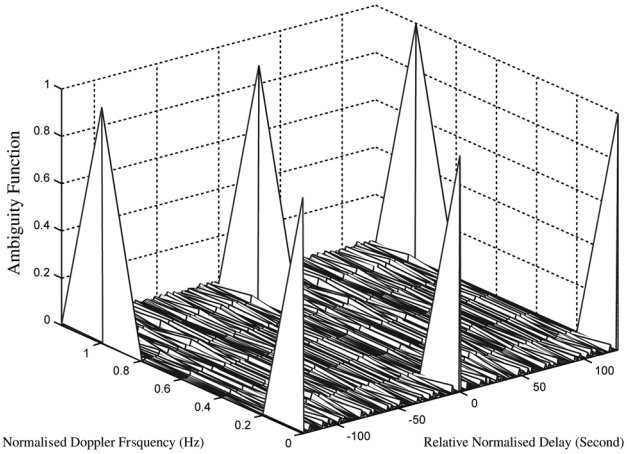


Fig. 5 *Periodic ambiguity function of a radar waveform modulated by a block cipher generated phase-code with length of 127 bits*

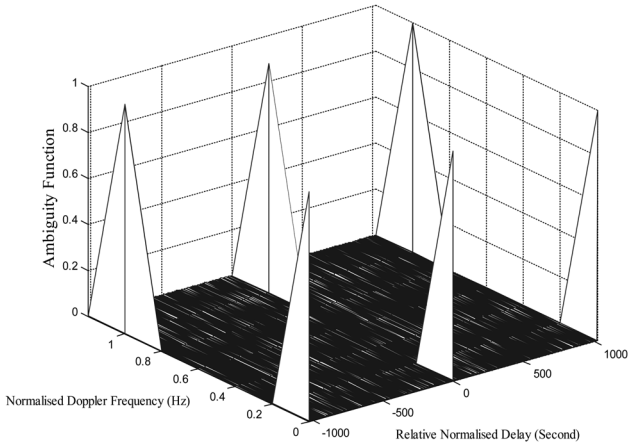


Fig. 6 *Periodic ambiguity function of a radar waveform modulated by a block cipher generated phase-code with length of 1023 bits*

Referring to (6), It should be mentioned that every target in a specific range gate, results in a mainlobe at normal delay of $k = 0$ and N–1 sidelobes at other range gates corresponding to normal delays of $k \neq 0$.

To discuss the maximum unambiguous range in condition of exploiting a block cipher output in phase-coded pulse compression, like any other pulse-radar, the 'pulse repetition frequency' (PRF) defines the maximum unambiguous range as

$$\text{Maximum Unambiguous Range} = \frac{c}{2 \times (\text{PRF})} \tag{36}$$

But in this article the block cipher key update time mentioned in section (5) should be taken into account to define the PRF. After key-update, all previous pulses sent by radar will not de-spread in radar receiver, hence we can say that average time of key-update has to be longer than pulse repetition interval. Thus according to (36), the following equation should also be noted to define the maximum unambiguous range

$$\text{Maximum unambiguous range} < \frac{c \times T_{\text{Key-update}}}{2} \tag{37}$$

Another useful criterion to measure receiver performance and define range and Doppler resolutions in radar waveform design is (periodic) ambiguity function which is denoted by $\chi(u; f_d)$ where u is normal delay matched on range resolution explained above and f_d is normalised Doppler frequency. An ideal waveform and matched filter, results in an ambiguity function which is centered at $\chi(0; 0)$ and is zero in other points. In other words, in an ideal system, all the energy of the matched filter output is centered for time and frequency mainlobes. Although this system is not practical at all, but it can be said that the more the ambiguity function of a waveform resembles to the ideal situation, the better the range and Doppler resolutions would be. Here in this section, computer simulations are used to plot and present the periodic ambiguity function of two block cipher generated phase-codes one with length of 127 bits in Fig. 5 and the other with length of 1023 bits in Fig. 6.

By comparing Fig. 4 with Fig. 5, it is obvious that the ambiguity function of a block cipher generated phase-code of length 1023 bits is much better than the length of 127 bits because it is more centered at $\chi(0; 0)$.

7 Conclusion

In this article, the importance of the security of a phase-code employed in radar pulse compression in the presence of ELINT and ES was defined. After reviewing some security features of a phase-code, we proposed the use of the output of a block cipher as phase-code. Next, we investigated the autocorrelation properties of such codes by ISR and PSR and some mathematical equations were also derived. To verify the equations, computer simulation results were presented to compare the proposed method with M-sequences. It was shown that despite the fact that M-sequences have better autocorrelation properties, but in practical radar systems with large value of pulse compression gain, this difference is not determinative with respect to other sources of interference such as AWGN or clutter. Afterwards, the probabilities of false alarm and detection in condition of using block cipher generated phase-codes were investigated and mathematical equations were presented along with simulation results. It was proved that there must be a relation between SNR and TNR in case of using a block cipher generated phase-code. Finally, to counter the important effect of repeater jammers and DRFMs, a key update method was introduced and a proper key update time was also derived. It was shown that by key update, a low probability of identification radar can be obtained and also simulation results proved that the jamming margin against repeaters was enhanced dramatically. Finally, range resolution, maximum unambiguous range and periodic ambiguity function of the mentioned method were discussed.

8 References

1 Headquarters, Department of the Army: 'FM 3-36; Electronic warfare' (Department of the Army, 2012), pp. 7–17
2 Skolnik, M.: 'Radar handbook' (The McGraw-Hill Book Companies, 1970, 3rd edn. 2008)
3 Butt, F.A., Jalil, M.: 'An overview of electronic warfare in radar systems'. TAEECE Int. Conf. on Advances in Electrical, Electronics and Computer Engineering, May 2013, pp. 213–217

4 Thingsrud, O.: 'DRFM-modulator for HRR-jamming'. RTO-MP-SET-080, October 2004, NATO Research Center
5 Rivest, J.F., Rajan, S.: 'Morphological detectors for radar ELINT applications'. IEEE Int. Conf. on Instrumentation and Measurement Technology, May 2013, pp. 1062–1067
6 Richards, M.A., Scheer, J.A., Holm, W.A.: 'Principles of modern radar' (SciTech Publishing, 2010)
7 Pace, P.E.: 'Detecting and classifying low probability of intercept radar' (Artech House Publications, 2009)
8 Thayaparan, T., Dakovic, M., Stankovic, L.J.: 'Mutual interference and low probability of interception capabilities of noise radar', *IET Radar Sonar Navig.*, 2008, **2**, (4), pp. 294–305
9 Adamy, D.L.: 'Electronic warfare modeling and simulation' (Artech House Publications, 2003)
10 Peterson, R., Ziemer, L., Borth, D.: 'Introduction to spread spectrum communications' (Prentice-Hall Publications, 1995)
11 Tafaroji, M., Falahati, A.: 'Improving code division multiple access security by applying encryption methods over the spreading codes', *IET Commun. J.*, 2007, **1**, (3), pp. 398–404
12 Sutton, R.: 'Secure communication, application and management' (John Wiley & Sons, 2002)
13 Hemanns, F.: 'Secure and robust tactical communications based on code-hopping CDMA'. RTO-MP-IST-083, April 2008, NATO Research Center
14 Golomb, S.: 'Signal design for good correlation for wireless communication, cryptography and radar' (Cambridge University Press, 2005)
15 Peebles, P.Z.: 'Radar principles' (John Wiley & Sons Inc., 1998)
16 Schneier, B.: 'Applied cryptography, protocols, algorithms and source codes in C' (John Wiley & Sons, 1996, 2nd edn. 2001)
17 Proakis, J., Salehi, M.: 'Fundamentals of communication systems' (Prentice Hall, 2004, 2nd edn. 2005)

doi: 10.1049/iet-rsn.2014.0066