Design and Implementation of Secured Digital Transceiver using Code-Shifted Reference Algorithm

[1]Ajeeth Kumar S, [2]Dakshinamoorthy R [3]Saranya T V
[1]Student, [2]Student, [3]Assistant professor
[1]Electronics and Communication Engineering
[1]Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, India

Abstract: This paper deals with the designing and implementation of digital code-shifted reference (CSR) transceiver in the hardware. By changing the physical properties of the transmission, the security of the transmission is improved without the help of higher level security options. CSR provides a simple manipulation of the physical property of the transmitting data without the use of precise timing device and multiple oscillators. The CSR transceiver helps us to transmit and receive the data using the help of security added to the transmitting data, which will protect the data from eavesdropping. The design of the transceiver is implemented in custom developed field-programmable gate array and the corresponding outputs are simulated.

***Index Terms*—Code-shifted reference(CSR), transceiver, field-programmable gate array (FPGA).**

I. Introduction

For applications in which sensitive data has to be handled by the transceiver, a robust protection must be provided from both passive and active potential adversaries. The active adversary deals with the creation of a transceiver which will send its own messages to the receiver by acting as a transmitter. The passive adversary is stealing of the information from the transmitter send to the receiver by acting like a receiver. Hence the addition of the security scheme is to reduce the stealing of information and also creation of similar transmitter.

The security of the data in [1] is based on the separation of the data and the reference from the receiver data, which can only be done by a legitimate receiver that is capable of locating the exact reference code for separating the data. For interpreting the data received by the receiver, the receiver must use an exact timing delay. It is difficult to design a precise timing delay in the hardware, especially with strict area limitations. In the code-shifted reference(CSR) scheme [2], [3] the data code is added with the reference code before it is transmitted. Orthogonal codes allow separation of the data code and the reference code in the code domain only by using a legitimate receiver. Hence, physical properties of the CSR scheme in [1] cannot be manipulated to resemble the security provided.

By using the energy collection method [6], a compact and low complexity architecture is designed for the CSR transceiver as a non-coherent transceiver [5]. Additional inherent security is provided by choosing the CSR scheme. Before the inclusion of the security key, the low possibility of detection and the masking of the number of bits transmitted simultaneously are basic properties of the code shifted reference. By including the security key into the CSR scheme provides higher security by allowing the only legitimate receiver to know how to separate the data code and the reference code that are received by the receiver.

The Sections of this article is given as follows. Section II describes the use of the orthogonal code and the CSR modulation scheme used for the transmitter algorithm. Section III presents the hardware implementation of the CSR transmitter and its operations. The receiver operation and its hardware architecture are explained in the Section IV and V. Section VI deals with the remarks and the conclusion of the CSR transceiver.

II. CSR Transmitter algorithm

In the transmitter and receiver orthogonal shifting codes are used to separate the reference code from the data code without any error. The transmitter and the receiver should agree with the shifting and the reference code used while transmitting the data. These matrices are composed of positive and negative ones for simulation and zeros and ones for hardware implementation. For the receiver to detect the transmitted data, the codes must shift the data orthogonally which must apply the following three conditions:

$$\sum_{i=0}^{N_f-1} \hat{c}_{ik} = 0, \quad \forall k \in \{1,2,\dots,M\}, \qquad (1)$$

$$\sum_{i=0}^{N_f-1} \hat{c}_{ik} c_{i0} c_{il} = \begin{cases} 0, & \text{if } k \neq l, \\ N_f, & \text{if } k = l, \end{cases} \forall k,l \in \{1,2,\dots,M\}, \qquad (2)$$

$$\sum_{i=0}^{N_f-1} \hat{c}_{ik} c_{il} c_{in} = 0, \qquad \forall k, l, n \in \{1, 2, \dots, M\}, \tag{3}$$

where C_{il} and C_{in} represent the possible shifting code, $\hat{C}_{ik}$ represents the code generated by multiplying the reference code with the shifting code, and C_{i0} represents a reference code. N_f and M represents the number of frames used and the number of bits added with the reference code, respectively. Multiple detection codes will be detected by changing the reference code and the shifting code continuously which should satisfy the conditions mentioned above. Reference code and the shifting code are obtained from the Walsh code which gives orthogonal codes. The detection code that are generated from the reference code and the shifting code will also satisfies the three conditions mentioned above.

For shifting the data in the code domain, the transmitted bit is multiplied with the shifting code so that each bit which are received will be shifted. If the codes are sent as pulse the reference code and the data are separated in code domain and will be combined in the time domain. The Walsh code is used for shifting the data since the Walsh code are orthogonal codes. In both the reference matrix and the shifting matrix, each code is orthogonal to each other. In the group there must be one orthogonal code and one reference code present during the transmission and the reception of the bits.

For transmission of the bits as a pulse, each code must be of same length since it will be converted as one symbol period from the number of frames. The symbol period represents the time required to simultaneously transmit a group of bits to the receiver. A group of N bits can be simultaneously transmitted by using any of the N+1 orthogonal codes. The shifting code and the reference code are selected on the basis of the effect it shows on the transmitting output. This will reduce the detection of the code while transmission and helps in better synchronization at the symbol level.

Shifting Codes

$$\begin{bmatrix} C_1 \\ C_2 \\ C_3 \\ C_4 \end{bmatrix} = \begin{bmatrix} 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \end{bmatrix}$$

Reference Codes

$$\begin{bmatrix} C_5 \\ C_6 \\ C_7 \\ C_8 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \end{bmatrix}$$

If the bits are transmitted as pulses then the information of four bits will be sent as one symbol period which will increases the performance of the receiver. In this transmission eight frames of two-bit data are transmitted to the receiver which will also denotes the reference code for that transmission. The bits are orthogonal in code domain and while considering in time domain they are separated. The bits used for the reference and data are collected together as a single sample that makes a pulse used for transmission while using time domain.

While using the bits for transmission of data through time domain eight frames will be used for each pulse to represent the four bits which are being transferred. This will be similar to the pulse amplitude modulation in which the amplitude of the pulse denotes the respective values of the bits that are being transferred. But on considering only the code domain eight frames of 16 bits will be transferred to the receiver. Where each frame represents the scalar form of the code that has been converted using CSR. While comparing the code domain with the time domain, the pulse will be having a different amplitude to represent the bits that are generated by code shifting. There will be four different values which will represent an amplitude of the pulse, hence two bits will be required to differentiate the four different values that are generated from the CSR transmitter. Each possible outcome will generate a different output for each change in reference code.

Algorithm 1 CSR Transmitter Algorithm

```
for n = 0; n < 8; + + n do
    DataImpact = $B_1\, C_{1n} + B_2\, C_{2n} + B_3\, C_{3n} + B_4\, C_{4n}$;
    Ref Impact = $C_r \times \sqrt{M}$;
    Scalar = |DataImpact + Ref impact|;
    end for
```

IJCRT

Algorithm 1 show the process in which the transmitting data is changed using CSR scheme. In the algorithm *Bi* are multiplied by the kth element of the respective shifting code and *n* denotes the frame number. The multiplied values will be added together to obtain a data impact. M represents the number of data bits transmitted and the square root of that value will be multiplied with one of the reference code that has been taken from the Walsh code. This value will be added with the data impact to obtain the scalar value. Which will give the four possible values in 8 frames in the time domain. For code domain 16-bit value is obtained for representing the 8 symbols where each symbol is represented by 2 bits.

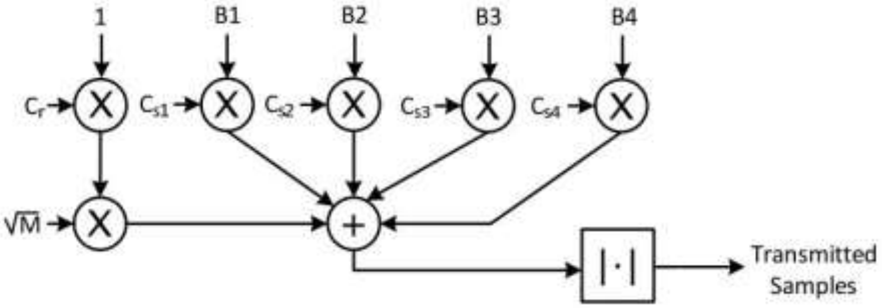

Fig. 1. Code-shifted reference transmitter

Fig. 1. Shows the CSR transmitter architecture. In which the data path will be multiplied with the data by the shifting code before adding the values to the reference code. The reference code does not change in the value hence one is multiplied then it will be multiplied with square root of the number of data bits that has to be transmitted. Now these values will be summed up together to obtain the bits that are going to be transmitted. The scalar values of these code are generated before the transmission of the bits. This scalar value can also be transmitted to the receiver through antenna as a waveform which are converted to pulse train for longer distance transmissions. The Synchronization of the reference code between the transmitter and the receiver is done by maintaining the same time delay for the right shift of the reference code which will allow the transmitter and the receiver to have the same reference code. The right shift will allow the reference code to shift one after the other in a cycle for using different reference code for different signals that are being transmitted to the receiver.

Algorithm 1 is applied below by using the data matrix *h* = [1 1 0 1] and reference C_6.

Code Shifted Data Matrix

$$\begin{bmatrix} C_1 \text{ x } h_0 \\ C_2 \text{ x } h_1 \\ C_3 \text{ x } h_2 \\ C_4 \text{ x } h_3 \end{bmatrix} = \begin{bmatrix} 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \end{bmatrix}$$

The square root of the length of the data array h is multiplied with one of the reference code, here C_6.

Reference Vector

$$[C_6 \text{ x } 2] = [\ 2 \quad 2 \quad -2 \quad -2 \quad -2 \quad -2 \quad 2 \quad 2\ ]$$

All the column value from the code shifted data matrix and the multiplied reference vector are added together to obtain the scalar matrix from which the absolute value will be obtained for the transmission of the bits. Where the resulting vector t represents the scalar value that are going to be transmitted to the receiver.

$$t = \begin{bmatrix} 4 & 0 & 0 & 4 & 0 & 4 & 0 & 4 \end{bmatrix}$$

By using the data code h results in the scaled values of zero and four. The absolute values restrict the presence of the negative values in the output. In addition to the restriction of positive values, the chosen Shifting code and the Reference code will produce the possible

IJCRT

outputs in the scalar values of zero, two, four and six. Which can be represented in the form of two-bit values.

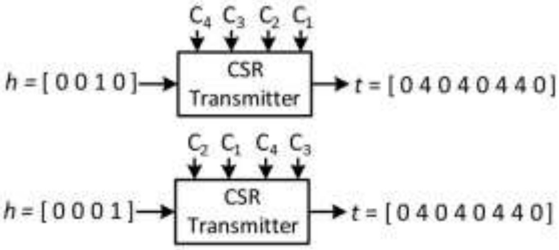

Fig. 2 Matching transmitter output.

The property of orthogonal code will limit the possibility of other outputs being generated at the transmitter. It will be helpful while the repetition of the data is present in the time domain for the separation of the inputs in code domain. These considerable outputs obtained from the transmitter are generated from the different shifting code and the reference code. By changing the shifting code and the reference code different set of output codes will be generated at the transmitter. For change in the shifting code for different inputs can produce same output as shown in Fig. 2. This can only be identified by the legitimate receiver having the security key. Hence only the intended receiver having the shared security key. By changing the shifting key and the reference key more different possibilities of the same input data will be obtained which will be difficult for the intruder to recover the data without the reference key. Hence without the reference code the perfect detection code cannot be generated which will increase the security to the data that has to be transmitted to the receiver and eavesdropping can be avoided or reduced to the maximum level.

The possibility of decoding the data that is transmitting can only be done by brute force, which is very much difficult while using CSR algorithm. Even if the eavesdropper knows the shifting code and the reference code of the transmitter. Each combination of the shifting code and the reference code will generate a similar scalar code for different input data. Since the reference code will be changing for every instance of time, without knowing the reference code used at that instance the possibility of recovering the data will be difficult.

In the worst-case scenario, the eavesdropper has prior knowledge about the reference code that has been using in the system. Which is hard for finding which reference code is used a specific time. This added more security to the physical property of the transmitting signal.

III. CSR Transmitter Architecture

For the implementation of CSR, the transceiver that has been designed only uses the security key for changing the reference code and the shifting code will not be changed which will reduce the multiplexer used for each bit transmitted and by keeping the shifting code constant the control logic of the security key is simplified.

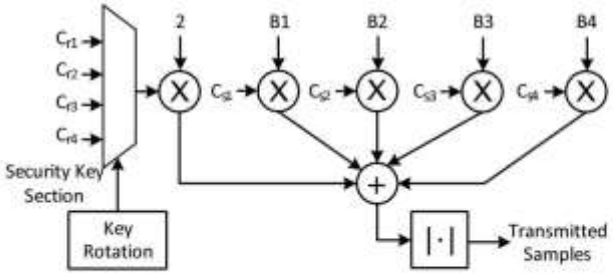

Fig. 3. Secure CSR transmitter architecture.

The architecture of secure CSR transmitter is show in Fig. 3. The reference code is determined by the security key which will create the reference code orthogonal to all the four bits transmitted simultaneously. A two-bit section of the security key denotes the four-possible reference code that are used for this implementation. the size of the transceiver is reduced by updating the reference code while reducing the overlapping occurring in the transmitter. While changing the reference code in the transmitter the detection code will also be changed in the receiver at the time of decoding the original data. Key Rotation seen in the Fig. 3 will act as the part of the security key which will change the reference code for every symbol boundary. For each rotation of the security key the reference code will be varied which will provide a different set of reference impact in the transmitter.

Since a group contains four bits, a constant value of two is used as a multiplier with the reference code. Which will limit the orthogonal code and helps in simplification of designing the transmitter. As the reference code is always positive or negative one. While multiplying the code will be positive or a negative two during the generation of the reference code in the simulation and hence it will be easier to represent the two possible outcomes using one or zero as a single bit value. Which can be represented as one for positive value of two and zero of negative value of two.

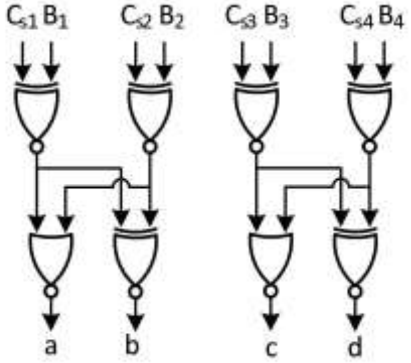

Fig. 4. Combinational logic for the reduction of the multiplier bank and first round of addition.

Fig. 4 shows the combinational logic made of XNOR gates and NOR gates to replace the multipliers and the two-adder required for the addition of the multiplication results together in the transmitter side. To reduce the transmitter complexity, the shifting code and the reference code are represented as single bit using zero instead of negative one. In the top row, each of the XNOR gate takes one of the shifting code and one bit from the group of bits that are going to be transmitted. The possible inputs to the multiplier are positive one and negative one which will reduce the possibility of the inputs to one or zero which is a one-bit value. The addition of the multiplied results will be positive two or negative two or zero. Even there are three possibilities of output is there, two bits are enough to represent the result of the added values in the time domain. In code domain 16-bit value is generated for transmitting the data to the receiver.

The scalar value is obtained by adding both the two-bit results from the multiplier and from the replacement values of a, b, c and d with the single bit e from the reference which is selected by using the security key which is show in the Fig 5. The combination logic is designed with the reduction of the two adders required for the addition of the multiplied result where e denotes the impact value. The output is taken as an absolute two-bit value of scalar form which will scale the values of zero, two, four and six as two-bit values. The table shows that the values of the possible two-bit values represents the four possible values that are generated using the CSR algorithm.

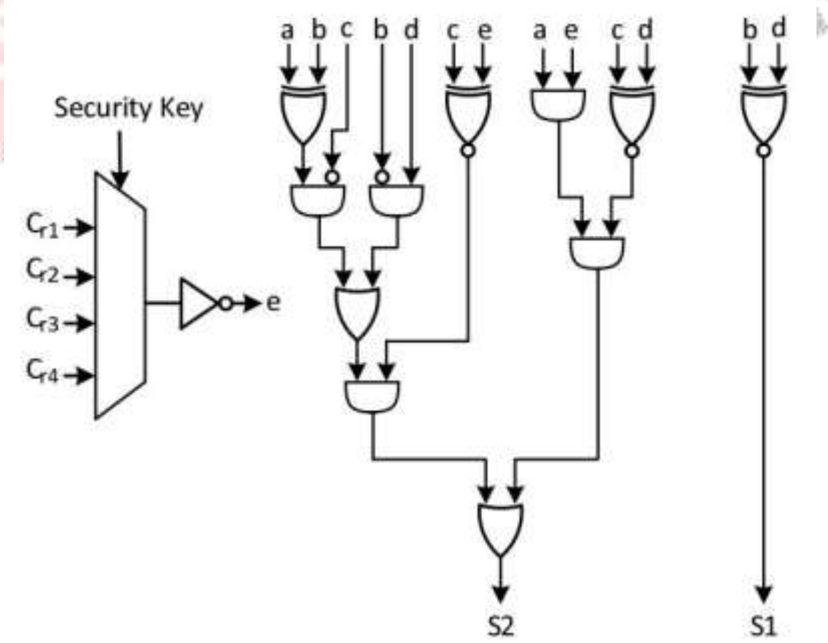

Fig. 5. Adder reduction data path.

IV. CSR Receiver Algorithm

For obtaining the received bit which are transmitted, at the receiver detection code is generated which will be used for decoding the received bits. As shown in the Algorithm 2, the detection code is the multiplied bits of the shifting code and the reference code. The reference code is synchronized with the transmitter from which the reference code will be selected from the reference matrix. Since 8 bits has to be recognized to obtain the 4-bit value in the code domain the detection code will be generated as a maximum of 4 cross 8 matrix. Synchronization is done by synchronized time difference at transmitter and the receiver.

Algorithm 2 CSR Receiver Algorithm

```
for $k = 0; k < 8; + + k$ do
    $D_1 = C_r C_{1k}; D_2 = C_r C_{2k};$
    $D_3 = C_r C_{3k}; D_4 = C_r C_{4k};$
    for $j = 0; j < BitLength; + + j$ do
        $Total = Total + Samples[j];$
    end for
    $SymTotal1 = SymTotal1 + (Total \times D_1);$
    $SymTotal2 = SymTotal2 + (Total \times D_2);$
    $SymTotal3 = SymTotal3 + (Total \times D_3);$
    $SymTotal4 = SymTotal4 + (Total \times D_4);$
end for
$B_1 = sign(SymbolTotal1);$
$B_2 = sign(SymbolTotal2);$
$B_3 = sign(SymbolTotal3);$
$B_4 = sign(SymbolTotal4);$
```

The received transmitted bit t will be squared and it is multiplied with the detection code which has been already generated by the receiver. In this case the reference code C6 is taken, which is multiplied with the shifting code. The following matrix shows the detection code for C6.

Detection code

$$\begin{bmatrix} C_1 \text{ x } C_6 \\ C_2 \text{ x } C_6 \\ C_3 \text{ x } C_6 \\ C_4 \text{ x } C_6 \end{bmatrix} = \begin{bmatrix} 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \end{bmatrix}$$

The array r is multiplied with the detection code which is shown in the following matrix.

$$\begin{bmatrix} D_1 \text{ x } r \\ D_2 \text{ x } r \\ D_3 \text{ x } r \\ D_4 \text{ x } r \end{bmatrix} = \begin{bmatrix} 16 & 0 & 0 & -16 & 0 & 16 & 0 & 16 \\ 16 & 0 & 0 & 16 & 0 & 16 & 0 & -16 \\ 16 & 0 & 0 & -16 & 0 & -16 & 0 & -16 \\ 16 & 0 & 0 & 16 & 0 & -16 & 0 & 16 \end{bmatrix}$$

The summed rows of the matrix are checked for the sign bit. If the addition of the rows gives the positive result then the bit is logic one and if the addition gives the negative result then the bit is logic zero. By taking sum for each row and checking for sign bit gives the transmitted bit to the receiver which is given by h = [1 1 0 1].

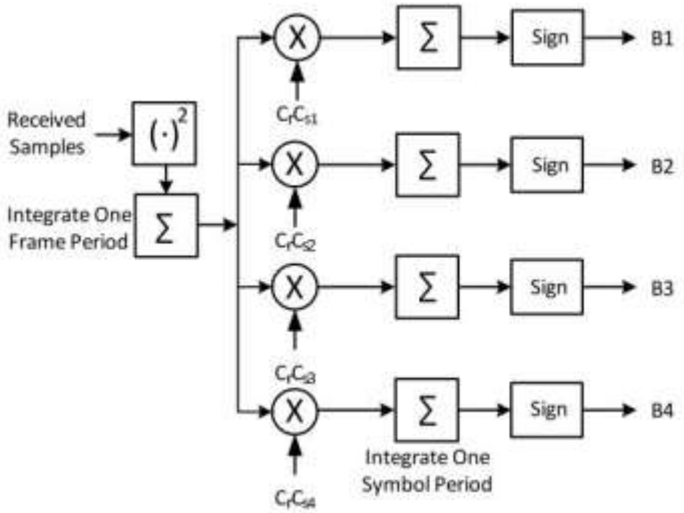

Fig. 6. Block diagram of the CSR decoder.

V. CSR RECEIVER ARCHITECTURE

In the hardware implementation of the CSR receiver the 16-bit values of detection code are generated in code domain, since it requires to decode the transmitted data of 16-bit design. The detection code is generated and 4 rows of 32-bit matrix is generated by the multiplication of the detection code and the received code. The 32 bit represents the two 16-bit values which are added together to obtain a set of 3-bit values. Further the 3-bit values are put into XOR operation to obtain the respective data matrix as the output.

VI. CONCLUSION AND FUTURE WORK

The Digital Secure Code Shifted Reference transceiver design and implementation was presented. Since physical layer properties are changed there will be less limitation in complexities, such as precise timing and use of multiple oscillators. The separation of the reference code and the data code requires more number of possible distributions to find the exact data that has been transmitted, hence it will difficult for eavesdropping without knowing which reference key is used during the transmission.

The Designed transceiver model is capable of transmitting and receiving the signal with an UART connection between two Xilinx devices allowing us to switch between transmitter and receiver using the control signal. This design helps in both transfer of data and the reception of data in a single device. The BER of the CSR algorithm is given in [7] which verifies the less production of bit error rate.

In future, CSR algorithm can be used for applications where Ultra-Wide Band frequencies are used for transmitting the data in time domain. This will give additional security and it will be suitable for the transmitting data at high speed. For applications where more security is needed at the physical property can apply CSR algorithm for data security. Further synchronization can be applied to the transceiver for better performance evaluation.

REFERENCES

[1] M.Ko and D. L. Goeckel, "Wireless physical-layer security perfor-mance of UWB systems," in *Proc. Military Commun. Conf*., Oct. 2010, pp. 2143–2148.

[2] H. Nie and Z. Chen, "Code-shifted reference transceiver for impulse radio ultra-wideband systems," *Phys. Commun*., vol. 2, no. 4, pp. 274–284, Dec. 2009.

[3] K. Aldubaikhy, "Differential code-shifted reference impulse-radio ultrawideband receiver: Timing recovery and digital implementation," M.S. thesis, Dept. Appl. Signal Process., Halifax Regional Municipality, NS, Canada, 2012.

[4] H. Nie and Z. Chen, "Performance analysis of code-shifted reference UWB radio," in *Proc. IEEE Radio Wireless Symp*., Jan. 2009, pp. 396–399.

[5] S. Vitavasiri, "A non-coherent ultra-wideband receiver: Algorithms and digital implementation," M.S. thesis, Dept. Elect. Eng. Comp. Sci., Massachusetts Inst. Technol., Cambridge, MA, USA, 2007.

[6] A. Hennessy, "Implementation of physical layer security of an ultrawideband transceiver," M.S. thesis, Dept. Elect. Eng., San Diego State Univ., San Diego, CA, USA, 2016.

[7] H. Nie and Z. Chen, "Performance evaluations for differential codeshifted reference ultra-wideband (UWB) radio," in *Proc. IEEE Int. Conf. Ultra-Wideband*, Sep. 2009, pp. 274–278.