Received 1 July 2014; revised 2 October 2014; accepted October 20, 2014. Date of publication 5 November, 2014;
date of current version 6 March, 2015.

*Digital Object Identifier 10.1109/TETC.2014.2367415*

# A Cross-Layer Secure Communication Model Based on Discrete Fractional Fourier Fransform (DFRFT)

**HONG WEN[1,2], JIE TANG[2], JINSONG WU[3], HUANHUAN SONG[2], TINGYONG WU[2], BIN WU[4], (Member, IEEE), PIN-HAN HO[1], SHI-CHAO LV[5], AND LI-MIN SUN[5]**

[1]Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada
[2]National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu 610051, China
[3]Department of Electrical Engineering, Universidad de Chile, Santiago 833-0072, Chile
[4]School of Computer Science and Technology, Tianjin University, Tianjin 300072, China
[5]Beijing Key Laboratory of IOT Information Security Technology, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100190, China

CORRESPONDING AUTHOR: H. WEN (h5wen@uwaterloo.ca)

This work was supported in part by the National Natural Science Foundation of China under Grant 61032003, Grant 61271172, and Grant 61372085, in part by the Renewable Fuels Development Program under Grant 20120185110030, Grant 20130185130002, and Grant 20120185110025, in part by the Strategy Research Foundation for the Returned Overseas Chinese Scholars and State Education Ministry, and in part by the Innovation Program through the Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China, under Grant Y4Z0033102.

**ABSTRACT** Discrete fractional Fourier transform (DFRFT) is a generalization of discrete Fourier transform. There are a number of DFRFT proposals, which are useful for various signal processing applications. This paper investigates practical solutions toward the construction of unconditionally secure communication systems based on DFRFT via cross-layer approach. By introducing a distort signal parameter, the sender randomly flip-flops between the distort signal parameter and the general signal parameter to confuse the attacker. The advantages of the legitimate partners are guaranteed. We extend the advantages between legitimate partners via developing novel security codes on top of the proposed cross-layer DFRFT security communication model, aiming to achieve an error-free legitimate channel while preventing the eavesdropper from any useful information. Thus, a cross-layer strong mobile communication secure model is built.

**INDEX TERMS** DFRFT, physical layer security, cross-layer, security code.

## I. INTRODUCTION

Discrete fractional Fourier transform (DFRFT) is a generalization of the discrete Fourier transform (DFT) and has been applied in optics, quantum mechanics, and signal processing areas [1], [2]. Pei and Hsue [3] extended the DFRFT to propose multiple-parameter discrete fractional Fourier transform (MPDFRFT) which has all of the desired properties for fractional transforms [4]. They also exploited the multiple-parameter feature of DFRFT to serve as encrypting digital data via proposing the double random phase encoding. Amr [5] pointed out that all the building blocks in this scheme are linear, and hence, breaking this scheme via known plaintext attack, is equivalent to solving a set of linear equations. [6]–[10] proposed several approaches of digital image encryption based on the fractional Fourier transform and chaos.

Physical-layer security techniques, which are based on the Shannon secrecy model [11] are effective in resolving the boundary, efficiency and link reliability issues for mobile communications. The built-in security of the physical-layer is defined as the physical-layer transmissions which guarantee low-probability-of interception (LPI) based on transmission properties such as modulations, signals and channels, without resorting to source data encryption. Wyner [12], Csiszar and Korner [13] developed the concept of the wire-tap channel for wired links.

The double random parameters encoding method [3] in DFRFT system also can serve for LPI purpose, which

leads to an approach of the physical-layer security system building. Compared with other physical-layer security approaches in [14]–[17], DFRFT approaches do not require the redundant antennas and two way communications.

Reference [17] and [18] presented that the physical-layer security under the information-theoretic security models can achieve exponentially close to perfect secrecy in theory if suitably long codes are used for privacy amplification. There are no computational restrictions to be placed on the eavesdropper in physical-layer security system. However, the information theoretic security is an average-information measure. The system can be designed and tuned for a specific level of security e.g., with very high probability a block is secure, but it may not be able to guarantee security with probability 1.

In the other hand, the security in classical cryptography system is based on unproven assumptions regarding the hardness of certain computational tasks. Therefore, systems are insecure if assumptions are wrong or if efficient attacks are developed. So any deployment of a physical-layer security protocol in a classical system would be part of a ''layered security'' solution where security is provided at a number of different layers, each with a specific goal in mind. Innovative cross-layer security designs considering both physical-layer security and upper-layer traditional security techniques are desirable for wireless networks.

In this paper, we propose a cross-layer approach to enhance the security of wireless network for wireless environments. We combine cryptographic techniques implemented in the higher layer with the physical layer security scheme using random parameters flipping of DFRFT systems to provide security advantages for legitimate partners. The proposed scheme introduces a distort signal parameter instead of a general signal parameter for wireless networks based on DFRFT system [1]–[3]. The transmitter randomly flip-flops between the distort signal parameter and the general signal parameter for confusing the attacker. An upper-layer pseudo-random sequence will be employed to control the flip-flops process. In our approach the physical-layer can utilize upper-layer encryption techniques for security, while physical-layer security techniques can also assist the security design in the upper layers.

We still extend the advantages between legitimate partners building from the cross-layer scheme via developing the security codes on top of our cross-layer DFRFT security communication model, aiming to achieve an error-free legitimate channel while preventing the eavesdropper from any useful information (i.e., with an error probability of 0.5). Thus, a strong secure model is built.

The rest of this paper is organized as follows. In section 2, we introduce the concept of the discrete fractional Fourier transform. The detailed description of novel cross-layer secure architecture model is given in section 3. In section 4, the construction of security codes is reviewed. The security communications system model is descript in section 5. Section 6 describes the experiment setup and simulation. Finally, we conclude the paper in section 7.

## II. DISCRETE FRACTIONAL FOURIER TRANSFORM

In this Section, following the definition of the continuous fractional Fourier transform (FRFT) [19], the definition of the discrete fractional Fourier transform (DFRFT) is given.

### A. CONTINUOUS FRACTIONAL FOURIER TRANSFORM

The $p$th order FRFT of a time domain signal $x(t)$ is defined as [1]:

$$X_p(u) = \int_{-\infty}^{+\infty} K_p(u,t)x(t)dt \tag{1}$$

where $K_p(u,t)$ is kernel given by

$$K_p(u,t) = A_\alpha \exp\left[j\pi(u^2\cot\alpha - 2ut\csc\alpha + t^2\cot\alpha)\right] \tag{2}$$

in which $n$ is integer, $A_\alpha = \sqrt{1-j\cot\alpha}$, and $\alpha = p\pi/2$ is the rotation angle of FRFT, $p \neq 2n$. When $p = 0$, $X_p(u)$ is the signal $x(t)$ itself after FRFT. When $p = 1$, FRFT is the conventional Fourier transform (FT).

The inverse of an FRFT (IFRFT) with an order $p$ is the FRFT with order $-p$ according to the following relation:

$$x(t) = \int_{-\infty}^{+\infty} X_p(u)K_{-p}(t,u)du \tag{3}$$

### B. DISCRETE FRACTIONAL FOURIER TRANSFORM

Let $x(n)$ be a sampled periodic signal with a period $\Delta t$ and $n = -N, -N+1, \ldots, N$, in which $N$ is the sampling interval of the signal $x(n)$. If we have function $y(n) = x(n\Delta t)$, let $\Delta u$ is the sampled period of $y(n)$, the $p$th order discrete fractional Fourier transform (DFRFT) of $x(n)$ is given by [1]:

$$X_p(m) = \sum_{n=-N}^{N} K_p^{\alpha,\Delta t,\Delta u}(m,n)\,x(n) \tag{4}$$

where $K_p^{\alpha,\Delta t,\Delta u}$ is DFRFT transform matrix and defined as:

$$K_p^{\alpha,\Delta t,\Delta u} = \sqrt{\frac{|\sin\alpha| - j\,\mathrm{sgn}(\sin\alpha)\cos\alpha}{2M+1}} \times e^{\frac{j}{2}\cot\alpha m^2\Delta u^2} e^{-j\frac{\mathrm{sgn}(\sin\alpha)2\pi nm}{2M+1}} e^{\frac{j}{2}\cot\alpha n^2\Delta t^2} \tag{5}$$

in which $m = -M, -M+1, \ldots M$ where $M$ is the sampling interval of the function $y(n)$.

The inverse of an DFRFT (IDFRFT) with an order $p$ is the DFRFT with inverse rotation angle $-\alpha$ and alternating $\Delta u$, $\Delta t$ according to the following relation:

$$x(n) = \sum_{n=-N}^{N} K_p^{-\alpha,\Delta u,\Delta t}(n,m)X_p(m) \tag{6}$$

When $M = N, \alpha = \pi/2$, IDFRFT becomes the inverse of discrete Fourier transform (IDFT). When $M = N, \alpha = -\pi/2$, DFRFT becomes the discrete Fourier transform (DFT).

### C. OFDM SYSTEM BASED ON DFRFT

The orthogonal frequency division multiplexing (OFDM) systems based on the discrete fractional Fourier transform is introduced in [20]. In the system, the fast Fourier transform (FFT) and inverse of fast Fourier transform (IFFT) are the replaced by DFRFT and IDFRFT. Assuming the cyclic prefix (CP) length is $N_g$, the $m$th sample of the $n$th transmitted frame is given by

$$X_p^i(m) = \sqrt{\frac{N}{N+N_g}} \sum_{n=0}^{N-1} K_{p,i}^{-\alpha,\Delta u,\Delta t}(m,n)\, x^i(n) \qquad (7)$$

where $-N_g \le m < N$, $x^i(n)$ is the symbol to be sent, assuming that different symbols are independent and identically distributed with a zero mean and average power $\sigma^2 \cdot K_{p,i}^{-\alpha,\Delta u,\Delta t}(m,n)$ expresses the calculation elements in IDFRFT with sampling space in time domain, given by Eqs. (5) and (6), in which $\alpha = p \cdot \pi/2$, $p$ is the fractional factor of the transform, $\Delta u$ is the sampling space in fractional Fourier domain, and $\Delta u T_s = 2\pi\,|\sin\alpha|/N$. When $\alpha = \pi/2$, the system is traditional orthogonal frequency division multiplexing (OFDM) system.

Let $h(k,l)$ be the discrete expression of the channel impulse response (CIR). The power spectrum of the channel obeys classical power spectra, the cross-correlation function of CIR can be described as:

$$E\left[h(p,l_1)\cdot h(q,l_2)\right] = \sigma_l^2 J_0(2\pi\,\Delta t f_d)\,\delta(l_1 - l_2) \qquad (8)$$

where $\Delta t = |p-q|\cdot T_s$, $\sigma_l^2$ is the total power of the $l$th path. $J_0$ is the zero-order Bessel function of the first kind, $f_d$ is the maximum Doppler frequency shift, $\delta(\bullet)$ is a Kronecker delta function, $(\bullet)^*$ represents complex conjugate.

We assume that the frame synchronized at the $k$th sample of the $j$th received frame is written as:

$$r_j(k) = \sum_{i=-\infty}^{\infty} \sum_{n=-N_g}^{N-1} h_{i,j}(k, k-m)\cdot x_i(n) e^{i2\pi\varepsilon/N} + \omega(k) \qquad (9)$$

where $0 \le k < N$, $\omega(k)$ is complex additive white Gaussian noise (AWGN) and unit variance, $\sigma_k^2$, $\varepsilon = \Delta f N T_s$ is the frequency offset relative to the inverse of symbol duration, $\Delta f$ is the frequency offset. The CIR of the $(j(N+N_g)+n)T_s$ time and the $l_1 + (j-i)(N+N_g)th$ path is:

$$h_{i,j}(k,l) = h(j(N+N_g)+n,\, l+(j-i)(N+N_g))$$

After removing the CP, the transformed signals of DFRFT can be expressed as:

$$X_p^j(\hat{m}) = \sum_{n=0}^{N-1} K_{p,j}^{\alpha,\Delta t,\Delta u}(\hat{m},n)\cdot r_j(n), \qquad (10)$$

where $0 \le \hat{m} < N$.

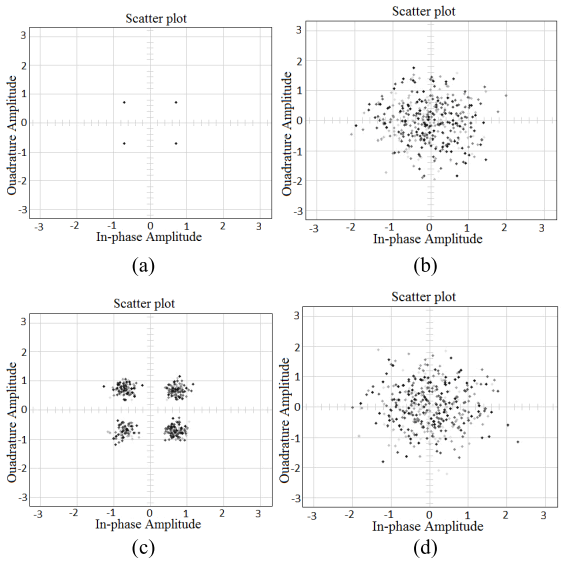



**FIGURE 1.** The signal constellation demodulation results with different parameters $\alpha$. The signal constellation before IDFRFT. (b) The signal constellation after IDFRFT. (c) The signal constellation after demodulation with $\alpha = 5°$. (d) The signal constellation after demodulation with $\alpha = 4.85°$.

## III. CROSS-LAYER SECURITY MODEL BASED ON DFRFT

In the DFRFT-OFDM system, the rotation angle $\alpha$ is one of the most important parameters. If the rotation angle $\alpha$ is 5° in the transmitter, the rotation angle $\alpha$ is 5° and 4.85° in the receivers, respectively. The error of demodulation is shown in Fig. 1, when the signal to noise ratio (SNR) is 0dB (error free). From Fig. 1 we can know that the correct signal constellation can be demodulated only and if only the rotation angle $\alpha$ is correctly known. Based on this fact, we introduce a distort signal parameter instead of a general signal parameter for the DFRFT-OFDM system. The transmitter randomly flip-flops between the distort signal parameter and the general signal parameter for confusing the attacker. An upper-layer pseudorandom sequence will be employed to control the flip-flops process.

In our scheme, two different rotation angles are denotes as $\alpha_1$ and $\alpha_2$ in the transmitter. An upper layer sequence set will be used to decide which rotation angle, either $\alpha_1$ or $\alpha_2$, is used to calculate the sending signal. Let the control sequence be $Q_{control} = (q_1, q_2, \ldots, q_n)$, $q_i \in GF(2)$. Then

$$\begin{cases} if \quad q_i = 0, & \alpha_1 \text{ is taken;} \\ if \quad q_i = 1, & \alpha_2 \text{ is taken.} \end{cases} \qquad (11)$$

The control sequence $Q_{control}$ will be the secret key stream between the transmitter and the intended receiver. An attacker does not know the control sequence $Q_{control}$, who possibly know the two different rotation angles $\alpha_1$ and $\alpha_2$. The attacker can not know when slot the rotation angle $\alpha_1$ or $\alpha_2$ will be taken, which illustrates the ambiguity in the conventional signal detector. The attacker will receive the signal using a random sequence instead of the control sequence $Q_{control}$. The attacker also can directly adopt the rotation angle $\alpha_1$ or $\alpha_2$ to perform demodulation.

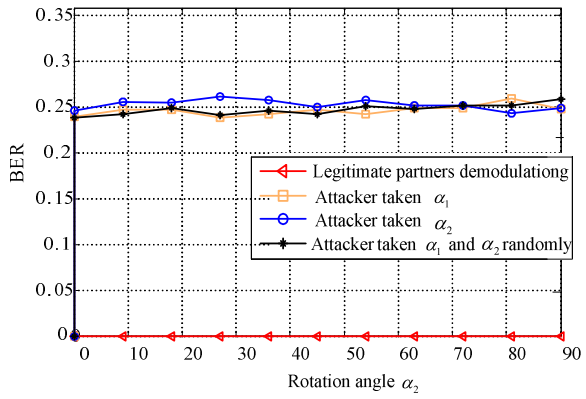



**FIGURE 2.** Received results of legitimate partners and attackers under $\alpha_1 = 0°$ with $\alpha_2$ changing from $\alpha_1$ to $\alpha_1 + 90°$.

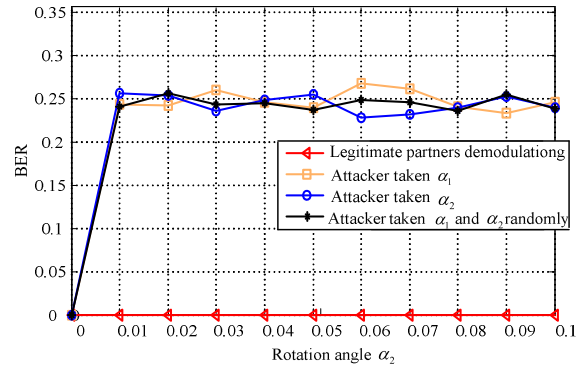



**FIGURE 3.** Received results of legitimate partners and attackers under $\alpha_1 = 0°$ with $\alpha_2$ changing from $\alpha_1$ to $\alpha_1 + 0.1°$.

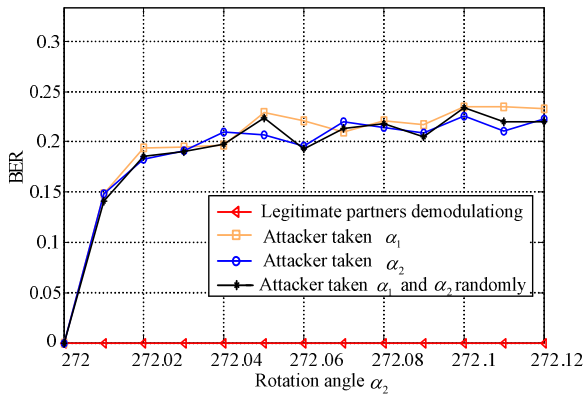



**FIGURE 4.** Received results of legitimate partners and attackers under $\alpha_1 = 272°$.

Fig. 2 to Fig. 4 illustrate the received results under perfect channel situation when the rotation angle $\alpha_1$ and $\alpha_2$ taken different values. In Fig. 2, the rotation angle $\alpha_1$ taken 0° and the rotation angle $\alpha_2$ will change from $\alpha_1$ to $\alpha_1 + 90°$. In Fig. 3 and Fig. 4 the rotation angle $\alpha_1$ takes 0°, and 272°, respectively while the rotation angle $\alpha_2$ will change from $\alpha_1$ to $\alpha_1 + 0.1°$. Even if the difference between $\alpha_1$ and $\alpha_2$ is very small, the legitimate partners may obtain the advantages over the attackers. From Fig. 2 to Fig. 4, we can know that the bit error rate (BER) of legitimate receivers approaches 0 when the BER of attackers is over 0.15 with the difference between $\alpha_1$ and $\alpha_2$ over 0.01.

## IV. SECURITY CODES CONSTRUCTION

### A. PRELIMINARIES

Obviously, the scheme described in the previous section goes only half-way to providing a strong security communication. After DFRFT randomly flip-flopping transmission, the legitimate partners have better receiving results than that of the attackers. Our motivation is to let error probability of attackers close to 0.5. Formally, let $M = \{m_1, m_2, \ldots, m_k\}$, $\hat{M} = \{\hat{m}_1, \hat{m}_2, \ldots, \hat{m}_k\}$ and $\hat{M}_E = \{\hat{m}_{E_1}, \hat{m}_{E_2}, \ldots, \hat{m}_{E_k}\}$ be vectors denoting transmitter's message, legitimate's received message and attacker's received message, respectively. The strong security is said to be achieved if the following relation holds:

$$\Pr(m_i \neq \widehat{m}_i) = 0$$
$$\Pr(m_i \neq \widehat{m}_{Ei}) = 0.5. \tag{12}$$

To achieve this goal, we need to develop the security codes (SC) that can further degrade the information received by attacker's without impairing the legitimate users.

### B. SECURITY CODES FROM RESILIENT FUNCTIONS

In [21], the novel constructions for generating security codes based on binary resilient functions [22], [23] are proposed, which serves as a systematic and practically implementable approach toward short code lengths and a low-complexity encoding/decoding process by taking advantage of matrix general inversion [25], [26]. We briefly review the results in [21]–[25] and [26] as follows.

### C. NOTATIONS OF BINARY RESILIENT FUNCTIONS

Resilient functions were firstly introduced and studied in [22]–[24], and were originally applied respectively to the key distribution and generation of random strings in presence of faulty processors. The definition of binary resilient functions is as follows.

*Definition 1 [22]:* Let $n \geq m \geq 1$ be integers and suppose:

$$f: \quad \{0,1\}^n \rightarrow \{0,1\}^m \tag{13}$$

where $f$ is a function that accepts $n$ input bits and produces $m$ output bits. Let $t \leq n$ be an integer. Suppose $(x_1, x_2, \ldots, x_n) \in \{0,1\}^n$, where $t$ arbitrary input bits out of $n$ are fixed by an adversary, and the remaining $n - t$ input bits are chosen independently at random. Then $f$ is said to be $t$-resilient by which an output of every possible $m$-tuple is equally likely to occur. Formally, the property can be stated as follows: Suppose $f(x_1, x_2, \ldots, x_n) = (s_1, s_2, \ldots, s_m)$ and let $(z_1, z_2, \ldots, z_n) \in \{0,1\}^n$ be an accepted input by an adversary. For every $t$-subset $(i_1, i_2, \ldots, i_t) \subseteq \{1, 2, \ldots, n\}$,

we have:

$$\Pr\left(f(z_1, z_2, \ldots, z_n) = (s_1, s_2, \ldots, s_m) \,|x_{ij} = z_{i_l}, 0 \le j, l \le t\right) = \frac{1}{2^m} \quad (14)$$

Such a function $f$ is called as a binary $(n, m, t)$ - resilient function.

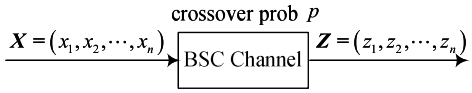



**FIGURE 5.** BSC with crossover probability $p$.

*Lemma 1:* Considering the model in Fig. 5, let $n$-tuple $\boldsymbol{X} = (x_1, x_2, \ldots, x_n)$ pass a BSC is shown in Fig. 5 and $\boldsymbol{Z} = (z_1, z_2, \ldots, z_n)$ be a noisy version of $\boldsymbol{X}$. Let $f$ be an $(n, m, t)$ - resilient function, i.e., $f(x_1, x_2, \ldots, x_n) = (s_1, s_2, \ldots, s_m)$. Let the channel crossover probability be $p$, i.e. $\Pr(x_i \neq z_i) = p$. We have:

$$p \ge \lim_{n\to\infty} \frac{(n-t)}{2n} \quad (15)$$

Let $(\tilde{s}_1, \tilde{s}_2, \ldots, \tilde{s}_m) = f(z_1, z_2, \ldots, z_n)$, then we have:

$$\Pr\left((\tilde{s}_1, \tilde{s}_2, \ldots, \tilde{s}_m) = (s_1, s_2, \ldots, s_m)\right) = \frac{1}{2^m} \quad (16)$$

*Lemma 2:* Let $(s_1, s_2, \ldots, s_m)$ in ***Lemma*** 1 be uniformly distributed over an $m$-tuple vector space. The average bit error rate (BER) for recovering message $(\tilde{s}_1, \tilde{s}_2, \ldots, \tilde{s}_m)$ from $\boldsymbol{Z} = (z_1, z_2, \ldots, z_n)$ is equal to 0.5, i.e., $Pr(\tilde{s}_i \neq s_i) = 0.5$, based on (15) and (16).

### D. PROPOSED BINARY SECURITY CODE CONSTRUCTION

In this subsection, we introduce a number of classes of security codes generated by binary linear resilient functions by taking advantage of matrix general inverse algorithms in [25] and [26].

Let function $f$ in (13) be a linear function, and $\boldsymbol{S}^T$ be the transpose of $\boldsymbol{S}$. $\boldsymbol{S} = (s_1, s_2, \ldots, s_m) = f(x_1, x_2, \ldots, x_n)$ can be denoted as:

$$\boldsymbol{S}^T = \boldsymbol{D}(x_1, x_2, \ldots, x_n)^T \quad (17)$$

where $\boldsymbol{D}$ is an $m \times n$ dimension matrix:

*Construction 1:* Let $\boldsymbol{D}$ be an $m \times n$ matrix from a $(n, m, t)$ resilient function. Let $\boldsymbol{G}$ be an $m \times n$ matrix such that $\boldsymbol{D} \cdot \boldsymbol{G}^T \cdot \boldsymbol{D} = \boldsymbol{D}$. Given $\boldsymbol{S} = (s_1, s_2, \ldots, s_m)$ as the secret information launched by the legitimate user, the encoding function on $\boldsymbol{S}$ should be:

$$\boldsymbol{X} = (x_1, x_2, \ldots, x_n) = \boldsymbol{S} \cdot \boldsymbol{G} + \boldsymbol{V} \quad (18)$$

where $\boldsymbol{V}$ is an arbitrary $n$ dimension vector such that $\boldsymbol{D} \cdot \boldsymbol{V}^T = \boldsymbol{0}$, and $\boldsymbol{X}$ is $(n, m)$ security code.

To derive $\boldsymbol{G}$, we firstly perform row and column permutations on $\boldsymbol{D}$:

$$\boldsymbol{D} = \boldsymbol{Q}_L \begin{bmatrix} \boldsymbol{I}_m & \boldsymbol{0} \end{bmatrix} \boldsymbol{Q}_R \quad (19)$$

where $\boldsymbol{I}_m$ is $m \times 1$ identity matrix, $\boldsymbol{0}$ is $m \times (n-m)$ all-zero matrix, $\boldsymbol{Q}_L$ and $\boldsymbol{Q}_R$ are $m \times m$ and $n \times n$ matrix, respectively. Note that such an operation can be performed only if $\boldsymbol{D}$ has a full column rank, i.e., $r = m$. where $r$ is the rank of $\boldsymbol{D}$. In this case $\boldsymbol{G}$ can be calculated as [25], [26]:

$$\boldsymbol{G}^T = \boldsymbol{Q}_R^{-1} \begin{bmatrix} \boldsymbol{I}_m & \boldsymbol{B} \end{bmatrix}^T \boldsymbol{Q}_L^{-1} \quad (20)$$

where $\boldsymbol{B}$ is $m \times (n-m)$ matrix and can be chosen randomly, which means $\boldsymbol{G}$ is not unique. Here we randomly choose one to calculate the encoded security information bits $\boldsymbol{S}$ as $\boldsymbol{S} \cdot \boldsymbol{G}$.

If $\boldsymbol{D}$ is not fully column ranked (i.e., $r < m$), $\boldsymbol{D}$ can be transferred into the form:

$$\boldsymbol{D} = \boldsymbol{Q}_L \begin{bmatrix} \boldsymbol{I}_r & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} \end{bmatrix} \boldsymbol{Q}_R \quad (21)$$

Then $\boldsymbol{G}$ can be calculated as:

$$\boldsymbol{G}^T = \boldsymbol{Q}_R^{-1} \begin{bmatrix} \boldsymbol{I}_r & \boldsymbol{B}_{12} \\ \boldsymbol{B}_{21} & \boldsymbol{B}_{22} \end{bmatrix} \boldsymbol{Q}_L^{-1} \quad (22)$$

where $\boldsymbol{B}_{12}$, $\boldsymbol{B}_{21}$ and $\boldsymbol{B}_{22}$ is a $r \times (m-r)$, $(n-r) \times r$ and $(n-r) \times (m-r)$ matrix, respectively, which can be chosen randomly to calculate $\boldsymbol{S} \cdot \boldsymbol{G}$.

If $\boldsymbol{D}$ has a full column rank, the rate of the secret code from **Construction** 1 is $r/n$.

One method in finding vector $\boldsymbol{V}$ in (18) is shown as follows. Let $\boldsymbol{D}_H$ be a $(n-m) \times n$ matrix such that

$$\boldsymbol{D}_H \cdot \boldsymbol{D}^T = \boldsymbol{0}, \quad (23)$$

where $\boldsymbol{0}$ represents an $(n-m) \times m$ all-zero matrix. Let $n-m$ by 1 vector $\boldsymbol{K}$ be randomly selected for computing $\boldsymbol{V} = \boldsymbol{K} \cdot \boldsymbol{D}_H$, which means that one source message $\boldsymbol{S}$ will correspond to numerous outputs $\boldsymbol{X}$ when a matrix $\boldsymbol{G}$ is given.

By launching $\boldsymbol{X}$ into the channel, the receivers will receive $\boldsymbol{Z} = (z_1, z_2, \ldots, z_n)$ which is the noisy version of $\boldsymbol{X}$. Decoding the secret information $= (\tilde{s}_1, \tilde{s}_2, \ldots, \tilde{s}_m)$ from $\boldsymbol{Z}$ yields

$$\tilde{\boldsymbol{S}} = (z_1, z_2, \ldots, z_n)\boldsymbol{D}^T \quad (24)$$

*Theorem 1:* A security code constructed via **Construction** 1 can avoid secret information $\boldsymbol{S}$ from leaking to any eavesdropper under BSC when the crossover probability of the wiretap channel is $p_w$ where $p_w \ge \lim_{n\to\infty} \frac{(n-t)}{2n}$. In other words, the error rate at the eavesdropper approaches to 0.5 if $p_w \ge \lim_{n\to\infty} \frac{(n-t)}{2n}$.

The proof of **Theorem** 1 directly follows by combining ***Lemma*** 1 with ***Lemma*** 2. We call this crossover probability $p_w$ as the *threshold probability*, and the corresponding security code is denoted as $(n, m, p_w)$.

## V. SECURITY SYSTEM MODEL

The secure communications model targeted in this study is shown in Fig. 6, where the source intends to send $m$ bits message $\boldsymbol{S} = \{s_1, s_1, \ldots s_m\}$ to the destination. Firstly, the source encodes the message such that

$$\boldsymbol{X} = \chi_1(\boldsymbol{S}) \quad (25)$$

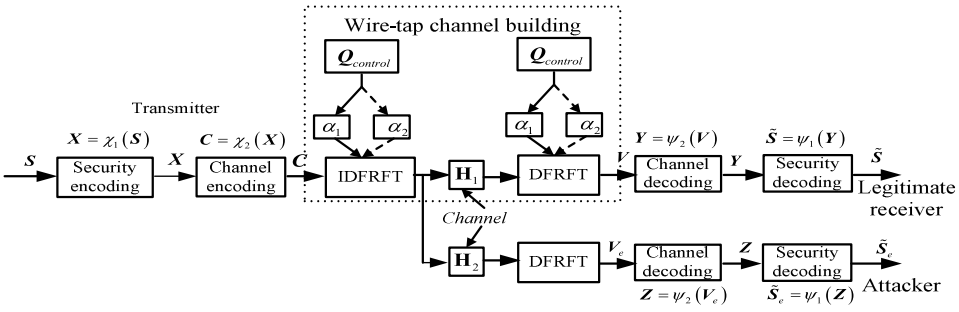



**FIGURE 6.** Security system model.

where $\chi_1$ is the security encoder function. Alice continues to encode $\boldsymbol{X}$ such that

$$\boldsymbol{C} = \chi_2(\boldsymbol{X}) \tag{26}$$

where $\chi_2$ is the channel encoder function. Then IDFRFT is performed under the control sequence $Q_{control}$. The sequence $\boldsymbol{V}$ received by the legitimate receiver is the noisy version of sequence $\boldsymbol{C}$. Meanwhile, an attacker can also observe the noisy sequence $\boldsymbol{V}_e$. the legitimate receiver performs DFRFT under the control sequence $Q_{control}$. The attacker performs DFRFT without the control sequence $Q_{control}$. Both the legitimate receiver and the attacker perform channel decoding as:

$$\boldsymbol{Y} = \psi_2(\boldsymbol{V}) \tag{27}$$

$$\boldsymbol{Z} = \psi_2(\boldsymbol{V}_e) \tag{28}$$

where $\psi_2$ is channel decoding function, which is an invertible function of the channel encoding function $\chi_2$. Then security decoding is performed as following:

$$\tilde{\boldsymbol{S}} = \psi_1(\boldsymbol{Y}) \tag{29}$$

$$\tilde{\boldsymbol{S}}_e = \psi_1(\boldsymbol{Z}) \tag{30}$$

where $\psi_1$ is security decoding function, which is an invertible function of security encoding function $\chi_1$.

## VI. SIMULATION RESULTS

### A. SECURITY CODE PERFORMANCE

The proposed **Construction** 1 is based on binary resilient functions $(n, m, d-1)$, which can be generated by a corresponding linear code $(n, m, d)$. In the experiment we implemented simplex codes $\left(2^m - 1,\ m,\ 2^{m-1}\right)$, which are the dual of Hamming codes, so as to yield a $\left(2^m - 1,\ m,\ 2^{m-1} - 1\right)$ linear resilient function. Fig. 8 shows the BER after applying the security codes versus the crossover probability $p$ of the BSC before applying the security codes.

### B. SECURITY SYSTEM PERFORMANCE

Corresponding to Fig. 2–Fig. 4, the security codes in Fig. 7 are put onto the cross-layer model under AWGN channel and Rayleigh channel. The WG stream ciphers [27] are employed to generate the control sequences. The security

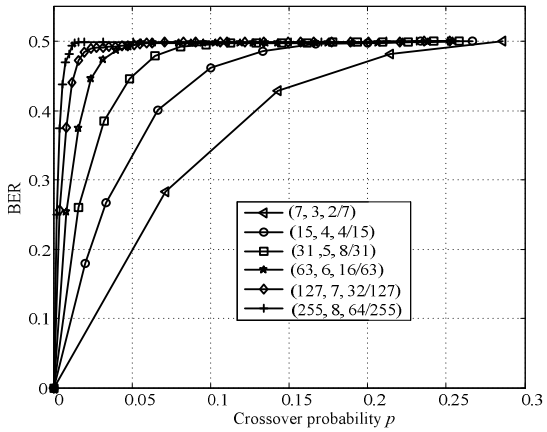



**FIGURE 7.** The performance of security codes generated by Construction 1 used simplex codes.

codes $(7, 3, 2/7)$, $(15, 4, 4/15)$ and $(31, 5, 8/31)$ are put on the top of the cross model in Fig. 2 to Fig. 4, respectively.

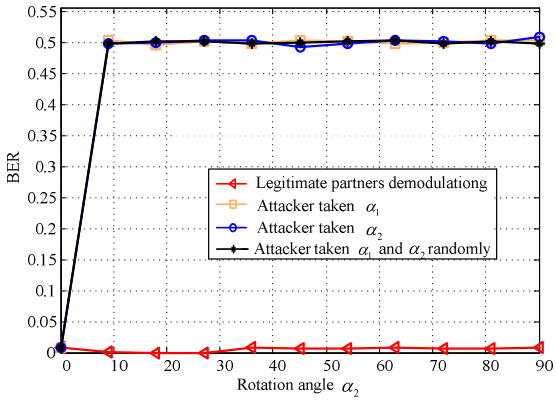



**FIGURE 8.** Received results of legitimate partners and attackers under $\alpha_1 = 0°$ with $\alpha_2$ changing from $\alpha_1$ to $\alpha_1 + 90°$.

Fig. 8 to Fig. 10 illustrate the received results when the rotation angle $\alpha_1$ and $\alpha_2$ taken different value after combining with security codes. In Fig. 8, the rotation angle $\alpha_1$ taken $0°$ and the rotation angle $\alpha_2$ will change from $\alpha_1$ to $\alpha_1 + 90°$. In Fig. 9 and Fig. 10 the rotation angle $\alpha_1$ taken $0°$, and $272°$, respectively while the rotation angle $\alpha_2$ will change from $\alpha_1$ to $\alpha_1 + 0.1°$. From Fig. 8 to Fig. 9, we can know that the BER of legitimate receivers are 0.007 to $2.016 \times 10^{-4}$ when

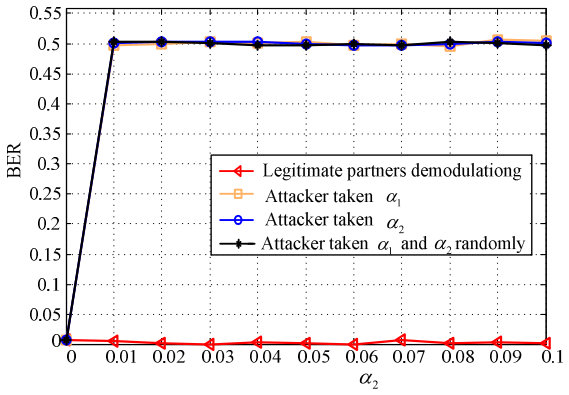



**FIGURE 9.** Received results of legitimate partners and attackers under $\alpha_1 = 0°$ with $\alpha_2$ changing from $\alpha_1$ to $\alpha_1 + 0.1°$.

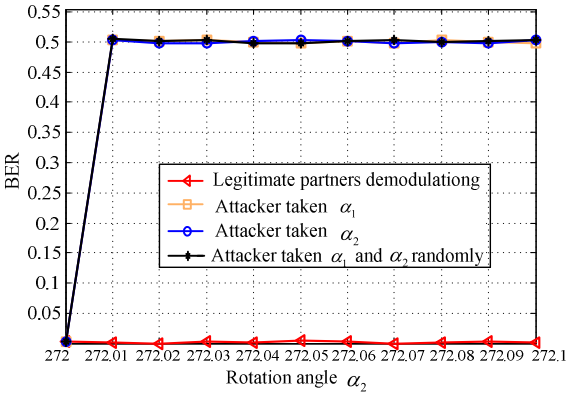



**FIGURE 10.** Received results of legitimate partners and attackers under $\alpha_1 = 272°$.

BER of attackers is approaching to 0.5, which means that the security system achieves almost error-free transmissions for the legitimate partners while zero information obtained by the attackers.

## VII. CONCLUSION

This paper has investigated the secure communications building via a cross-layer method based on DFRFT under Wyner's model. By combining cryptographic techniques implemented in the higher layer with the physical layer security scheme using random parameters flipping of DFRFT systems, where the channel advantage of the intended receiver is ensured first by DFRFT and IDFRFT processing controlled by higher layer cryptography. The advantages of the legitimate partners are continuously extended by developing the security codes on top of our cross-layer DFRFT security communication model. A strong secure model for mobile communications is built. The security codes generated from binary resilient function are with low complexity performance. The effectiveness of proposed scheme is demonstrated via simulation results.

## REFERENCES

[1] C. Candan, M. A. Kutay, and H. M. Ozaktas, "The discrete fractional Fourier transform," *IEEE Trans. Signal Process.*, vol. 48, no. 5, pp. 1329–1337, May 2000.

[2] Q.-W. Ran, H.-Y. Zhang, Z.-Z. Zhang, and X.-J. Sha, "The analysis of the discrete fractional Fourier transform algorithms," in *Proc. Can. Conf. Elect. Comput. Eng. (CCECE)*, May 2009, pp. 979–982.

[3] S.-C. Pei and W.-L. Hsue, "The multiple-parameter discrete fractional Fourier transform," *IEEE Signal Process. Lett.*, vol. 13, no. 6, pp. 329–332, Jun. 2006.

[4] A. Mostayed, K. Sikyung, and S. Z. K. Sajib, "Novel parameter estimation method for chirp signals using Bowtie Chirplet and discrete fractional Fourier transform," in *Proc. 2nd Int. Conf. Future Generat. Commun. Netw. Symp. (FGCNS)*, vol. 3. Dec. 2008, pp. 23–26.

[5] A. M. Youssef, "On the security of a cryptosystem based on multiple-parameters discrete fractional Fourier transform," *IEEE Signal Process. Lett.*, vol. 15, no. 1, pp. 77–78, Jan. 2008.

[6] R. Tao, X.-Y. Meng, and Y. Wang, "Image encryption with multiorders of fractional Fourier transforms," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 4, pp. 734–738, Dec. 2010.

[7] N. Jindal and K. Singh, "Image encryption using discrete fractional transforms," in *Proc. Int. Conf. Adv. Recent Technol. Commun. Comput.*, 2010, pp. 165–167.

[8] N. Ghoshal and J. K. Mandal, "Discrete Fourier transform based multimedia colour image authentication for wireless communication (DFTMCIAWC)," in *Proc. Int. Conf. Wireless VITAE*, Feb./Mar. 2011, pp. 1–5.

[9] E. H. Elshazly, M. A. Ashour, E. M. Elrabaie, and A. M. Abbas, "An efficient fractional Fourier transform approach for digital image watermarking," in *Proc. 29th Nat. Radio Sci. Conf. (NRSC)*, Apr. 2012, pp. 245–254.

[10] W. Yaqing and Z. Shangbo, "A novel image encryption algorithm based on fractional Fourier transform," in *Proc. Int. Conf. Comput. Sci. Service Syst. (CSSS)*, Jun. 2011, pp. 72–75.

[11] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no 4, pp. 656–715, 1949.

[12] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387. 1975.

[13] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[14] A. O. Hero, "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

[15] H. Koorapaty, A. A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Commun. Lett.*, vol. 4, no. 2, pp. 52–55, Feb. 2000.

[16] Y. Zhang and H. Dai, "A real orthogonal space-time coded UWB scheme for wireless secure communications," *J. Wireless Commun. Netw.*, vol. 2009, pp. 1–8, Sep. 2009.

[17] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[18] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1955.

[19] M. H. Ozaktas, O. Arikan, M. A. Kutay, and G. Bozdagt, "Digital computation of the fractional Fourier transform," *IEEE Trans. Signal Process.*, vol. 44, no. 9, pp. 2141–2150, Sep. 1996.

[20] M. Martone, "A multicarrier system based on the fractional Fourier transform for time-frequency-selective channels," *IEEE Trans. Commun.*, vol. 49, no. 6, pp. 1011–1020, Jun. 2001.

[21] H. Wen, P.-H. Ho, and B. Wu, "Achieving secure communications over wiretap channels via security codes from resilient functions," *IEEE Wireless Commun. Lett.*, vol. 3, no. 3, pp. 273–276, Jun. 2014.

[22] B. Chor, O. Goldreich, J. Hastad, J. Freidmann, S. Rudich, and R. Smolensky, "The bit extraction problem or t-resilient functions," in *Proc. 26th Annu. Symp. Found. Comput. Sci.*, pp. 396–407, Oct. 1985.

[23] C. H. Bennett, G. Brassard, and J. M. Robert, "Privacy amplification by public discussion," *J. Comput.*, vol. 17, no. 2, pp. 210–229, 1988.

[24] J. Bierbrauer, K. Gopalakrishnan, and D. R. Stinson, "Orthogonal arrays, resilient functions, error-correcting codes,and linear programming bounds," *J. Discrete Math.*, vol. 9, no. 3, pp. 424–452, 1996.

[25] S. L. Campbell and C. D. Meyer, *Generalized Inverses of Linear Transformations*. London, U.K.: Pitman, 1979.

[26] M. Z. Nashed, Ed., *Generalized Inverses and Applications*. New York, NY, USA: Academic, 1976.

[27] Y. Nawaz and G. Gong, "WG: A family of stream ciphers with designed randomness properties," *Inf. Sci.*, vol. 178, no. 7, pp. 1903–1916, 2008.

**HONG WEN** was born in Chengdu, China. She received the Ph.D. degree from the Department of Communication and Computer Engineering, Southwest Jiaotong University, Chengdu, in 2004. She was an Associate Professor with the National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu. From 2008 to 2009, she was a Visiting Scholar and Post-Doctoral Fellow with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. Her current main interests lie in wireless communication systems security.

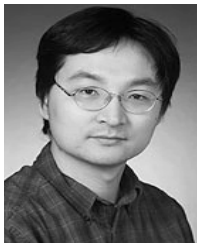
**JIE TANG** was born in Chengdu, China. He is currently pursuing the Ph.D. degree in communication and information system with the National Key Laboratory of Science and Technology on Communications, Chengdu. His current main interests lie in wireless communication system and information security.

**JINSONG WU** received the Ph.D. degree in electrical and computer engineering from Queen's University, Kingston, ON, Canada. He is currently an Associate Editor of the *IEEE Communications Surveys and Tutorials*, the *IEEE Systems Journal*, and the *IEEE Access*, and the Series Editor of the IEEE Series on Green Communications and Computing Networks for the *IEEE Communications Magazine*. He was the leading Editor of the comprehensive book entitled *Green Communications: Theoretical Fundamentals, Algorithms, and Applications* (CRC Press, 2012). He is currently with the Department of Electrical Engineering, Universidad de Chile, Santiago, Chile.

**HUANHUAN SONG** was born in Zaozhuang, China. She received the bachelor's degree from the Department of Electronic Information Science and Technology, Shandong Agricultural University, Tai'an, China, in 2012. She is currently pursuing the M.Sc. degree with the National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu, China. Her current main interests lie in cross-layer security for wireless communication systems.

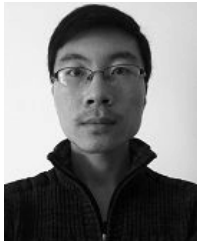
**TINGYONG WU** was born in Sichuan, China, in 1975. He received the B.Eng., M.Eng., and Ph.D. degrees from the University of Electronic Science and Technology of China, Chengdu, China, in 1998, 2001, and 2007, respectively, where he is currently an Associate Professor with the National Key Laboratory of Science and Technology on Communications. His current research interests include signal processing in wireless communication and statistical signal processing.

**BIN WU** (S'04–M'07) received the Ph.D. degree in electrical and electronic engineering from the University of Hong Kong, Hong Kong, in 2007. He was a Post-Doctoral Research Fellow with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, from 2007 to 2012. He is currently a Professor with the School of Computer Science and Technology, Tianjin University, Tianjin, China. His research interests include computer systems and networking, IP, optical and wireless communications and networking, and network survivability and security issues.

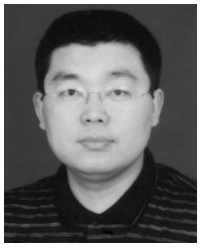


**PIN-HAN HO** received the B.Sc. and M.Sc. degrees from the Department of Electrical and Computer Engineering, National Taiwan University, Taipei, Taiwan, in 1993 and 1995, respectively, and the Ph.D. degree from Queen's University, Kingston, ON, Canada, in 2002.

He joined the Department of Electrical and Computer Engineering at the University of Waterloo, Waterloo, ON, Canada, as an Assistant Professor in 2002, where he is currently a Full Professor.



**SHI-CHAO LV** was born in Baoding, China. He received the M.A. degree from the National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu, China, in 2012. After his graduation, he joined as an Engineer at the State Key Laboratory of Information Security, Beijing, China, as a Researcher. After two year's work as a Security Engineer, he is currently pursuing the Ph.D. degree with the University of Chinese Academy of Sciences, Beijing. His major interests focus on wireless communication systems security.



**LI-MIN SUN** was born in Henan, China. He received the Ph.D. degree from the Department of Computer Science and Engineering, National University of Defense Technology, Changsha, China, in 1998. He was an Associate Professor with the Chinese Academy of Sciences, Beijing, China, where he is currently a Professor of Computer Science with the Institute of Information Engineering. His current main interests lie in wireless communication systems security.