Novel Hybrid Public/Private Key Cryptography Based on Perfect Gaussian Integer Sequences

CHING-HSIEN HSIA¹, SHI-JER LOU², HO-HSUAN CHANG³ and DONGHUA XUAN³

¹Department of Industrial Technology Education, National Kaohsiung Normal University, Kaohsiung, Taiwan.
²Graduate Institute of Technological and Vocational Education, National Pingtung University of Science and Technology, Pingtung, Taiwan.
³Information Engineering College, Guangzhou City Construction College, Guangzhou City, Guangdong Province, China.

Corresponding author: Ho-Hsuan Chang (e-mail: 3500916355@qq.com).

ABSTRACT This paper proposes a novel hybrid public/private key cryptography scheme based on perfect Gaussian integer sequences (PGISs) of period \( N = pq \). First, a review study of construction degree-4 PGIS is addressed. We show that circular convolution over PGISs is a trapdoor one-way permutation function that enables simultaneous cipher encryption and digital signatures. To implement the proposed cipher encryption scheme, a private PGIS is assigned as the encryption key sequence for circular convolution with the plaintext to generate the ciphertext. The reverse decryption key sequence involves the time reflection and complex conjugation of the encryption sequence, which can be regenerated using a pair of public and private keys. The security level of the proposed scheme is the same as that of the Rivest-Shamir-Adleman (RSA) system; however, the capacity of a cryptosystem based on PGISs may outperform that of based on RSA, because the abundant PGISs are available. Simulation results show that the approximation error when finite digits are used to represent the irrational coefficients of a normalized PGIS can be relatively small compared with the noise. This contributes to the simplicity of this scheme’s implementation. With the fast development of IoT (internet of things), the adaptation and applicability of the proposed scheme to IoT platforms are also addressed, where lightweight cryptographic functions are preferable due to the limited resources of IoT devices.

INDEX TERMS Cryptography, encryption, PGIS, RSA, trapdoor one-way function.

I. INTRODUCTION Encryption is the process of converting ordinary information (plaintext) into unintelligible text (ciphertext), which can be read only if decrypted. A cipher is a pair of algorithms that encrypt the plaintext and decrypt the ciphertext. The operation of a cipher is controlled by the algorithm and by a key in each instance. Cryptosystems are categorized into two types: symmetric and asymmetric. In symmetric systems, the same private key is used to encrypt and decrypt a message. Asymmetric systems use a public key to encrypt a message and a private key to decrypt it. Symmetric models include one-time pad, the commonly used advanced encryption standard (AES), which replaced the older data encryption standard (DES) [1], etc. Asymmetric systems include the Rivest-Shamir-Adleman (RSA) algorithm [2], the Diffie-Hellman key exchange algorithm [3], the digital signature standard [4], and the elliptic curve cryptography [5], [6].

Public-key cryptography does not require a secure channel for the initial exchange of one (or more) secret keys; thus, it is often used to secure electronic communication over an open network environment such as the Internet. By contrast, symmetric cryptosystem encounters private key distribution and management problem, in which the cost and delay imposed by key distribution are major barriers to the transfer of business communications to large networks or the Internet. With the rapid development of the Internet and the high demand for secure communications across public networks, public-key cryptography has attracted much more attention than private-key cryptography because of its affordability. The development of public-key cryptography originated with the trapdoor one-way concept introduced by Diffie and Hellman [3]. However, they did not present an example of how such a cryptosystem could be implemented. The search for a trapdoor one-way function was left as an open problem, rendering public-key encryption a fascinating theoretical discovery but unusable in practice. The factorization of a product of
two large prime numbers is an example of a trapdoor one-way permutation function. Although selecting and verifying two large primes and multiplying them together is easy, factoring the resulting product is very difficult. Motivated by the trapdoor one-way property of prime factorization, Rivest et al. implemented the first public-key cryptosystem, known as the asymmetric RSA cryptosystem [2].

In this paper, we show that circular convolution over perfect Gaussian integer sequences (PGISs) is also considered a trapdoor one-way function, and we create a novel cipher encryption and decryption scheme based on circular convolution and a set of PGISs. A sequence is regarded as perfect if it has an ideal periodic autocorrelation function (PACF), and a PGIS is a perfect sequence (PS) in which all elements are complex numbers, (i.e., \( a + bj \), where \( j = \sqrt{-1} \) and \( a \) and \( b \) are integers). To implement this scheme, an encryption key sequence is chosen from a set of PGISs of period \( N = pq \), where both \( p \) and \( q \) are odd primes, for circular convolution with plaintext of size \( N \) to generate a ciphertext. The encryption PGIS is kept private, and the decryption key is the time reflection and complex conjugation of the encryption PGIS. The public key consists of all information, except the private key number, which is required for generating the decryption PGIS at the receiver end. Because the private key number is available only to authorized users and can be shared by other means such as the Diffie-Hellman key exchange algorithm, the ciphertext cannot be encrypted by adversaries. The proposed scheme consists of both public and private keys, thus it is basically a public-key cryptography; however the public-key cryptography encounters no private key exchange problem. Comparing with the private-key cryptography, our scheme has the advantage that it requires only to share the private key number between two parties instead of the requirement of secure distribution of more complex decryption keys among authorized users. Therefore, it is considered a form of hybrid public/private key cryptography, and it can take the advantages of both two.

The construction of PGISs has become a prominent research topic [7]-[22], because their implementation is simpler than that of other PSs with real or complex coefficients. PGISs were applied to orthogonal frequency-division multiplexing (OFDM) systems for peak-to-average power ratio reduction [15] and were used to construct a transformation matrix for precoded OFDM systems to achieve full frequency diversity and an optimal bit error rate [16]. PGISs were also adapted as the frequency-domain comb-spectrum (CS) codes for a novel CS-CDMA system [17]. Recently, Chang developed a CDMA scheme based on PGISs, called the PGIS-CDMA system [18].

This is the first study to apply PGISs to a data encryption and decryption scheme, where the operation of data encryption is made through circular convolution. As addressed in Section VI, circular operation is considered a vector-wise operation rather than element-wise operation, where the vector-wise operation is more complex, but it can achieve higher level of confidentiality. This study begins with a review construction of a set of degree-4 PGISs of period \( N = pq \). In this construction, the degree of a sequence is defined as the number of distinct nonzero sequence elements within one period. The resultant set of PGISs is then applied in the proposed hybrid public/private key cryptography.

Here, the development of PGIS constructions is briefly introduced. A general form of even-period PGISs was presented in [7]. Yang et al. [8] constructed PGISs of an odd prime period \( p \) by using cyclotomic classes with respect to the multiplicative group of \( \text{GF}(p) \). Ma et al. [9] later presented PGISs with a period of \( p(p + 2) \) based on Whitman’s generalized cyclotomy of order two over \( \mathbb{Z}_{p(p+2)} \), where \( p \) and \((p + 2)\) are twin primes. Degree-3 and degree-4 PGISs of arbitrary composite periods were constructed by Chang et al. [10]. Lee et al. focused on constructing degree-2 PGISs of various periods using two-tuple-balanced sequences and cyclic difference sets [11]-[12]. Pei et al. developed algorithms that could generate PGISs of arbitrary periods [13]. A systematic method for constructing sparse PGISs in which most of the elements are zero appeared in [14]. Lee et al. constructed families of PGISs with high energy efficiency [19], [20]. PGISs of period \( p^k \) with degrees less than or equal to \( k + 1 \) were proposed in [21]. Chang et al. contributed a thorough study of constructing PGISs of period \( N = qp \), where \( p \) and \( q \) are two primes [22].

This paper is organized as follows. The definition and properties of PGISs are introduced in Section II. We present the review study of degree-4 PGIS construction of period \( N = qp \) for the proposed scheme in Section III, showing that there exist infinite PGISs of this period. We prove in Section IV that PGIS-based circular convolution is a trapdoor one-way permutation function. The implementation and digital signatures are addressed in Section V. In Section VI, the performance of RSA, other private-key cryptography and the proposed scheme are compared. An analysis of approximation that uses finite digits to represent the irrational coefficients of a normalized PGIS is presented in Section VII. In Section VIII, we analyze the adaptation and applicability of the proposed scheme to IoT (internet of things) platform. Finally, conclusions are drawn in Section IX.

II. PRELIMINARIES

A. DEFINITIONS OF PGIS

Let \( N = pq \), where \( p \) and \( q \) are distinct prime numbers. In addition, \( s = \{s[n]\}_{n=0}^{N-1} \) denotes a sequence of period \( N \), where \( s[n] \) is the \( n \)th component of \( s \). Let \( R_s = \{R_s[\tau]\}_{\tau=0}^{N-1} \) be the periodic autocorrelation function (PACF) of \( s \), i.e.,

\[
R_s[\tau] = \sum_{n=0}^{N-1} s[n]s^*[(n - \tau)_N],
\]

where the superscript * denotes the complex conjugate operation, and \( (\cdot)_N \) is the modulo \( N \) operation. Define \( s_{-1} = \{s((-n)_N)\}_{n=0}^{N-1} \), \( R_s = s \otimes s_{-1}^* \), where \( \otimes \) denotes the circular convolution operation. Let \( S = \{S[n]\}_{n=0}^{N-1} \) denote the discrete Fourier transform (DFT) of \( s \). The DFT of \( R_s \)
is then given by $S \circ S^* = |S|^2$, where $\circ$ and $| \cdot |$ denote the component-wise product operation and the Euclidean norm, respectively.

The sequence $s$ is said to be perfect if and only if it has an ideal PACF, i.e., $R_s = E \cdot \delta_N$, where $E = \sum_{n=1}^{N-1} |s[n]|^2$ is the energy of sequence $s$, and $\delta_N$ is a delta sequence of period $N$. The DFT pair relationship between $R_s = E \cdot \delta_N$ and $S \circ S^* = |S|^2$ indicates that a sequence $s$ is perfect if and only if the spectrum magnitude of $s$ is flat (i.e., $|S[n]| = \sqrt{E}, \ 0 \leq n \leq N - 1$).

**Theorem 1:** ([18]) In addition to the $N$-tuple $s = (0, \ldots, 0)$ and all $N - 1$ circular shifts, there are no other degree-1 PGISs of period $N$, where $a$ is a nonzero Gaussian integer.

**B. CONSTRUCTION AND PROPERTIES OF CIRCULANT MATRIX**

We define a circulant matrix $X$ of size $N \times N$ based on the sequence $x = \{x[n]\}_{n=0}^{N-1}$ of period $N$, where the elements of $x$ form the first column of $X$. With this definition, $X = \{x[(n - k)N]\}$, and the $(n, k)$ entry of $X$, denoted as $X_{n,k}$, is

$$X_{n,k} = x[(n - k)N].$$

Let $x(i) = \{x[(n - i)N]\}$ denote the circular shift of $x$ to the right by $i$ steps. Circulant matrix $X$ can be expressed using the matrix form as follows:

$$X = [x \ x^{(1)} \ x^{(2)} \ \cdots \ x^{(N-1)}].$$

The eigenvalues of a circulant matrix comprise the DFT of the first column of the circulant matrix, and conversely, the first column of the circulant matrix is the inverse DFT of the eigenvalues. In particular, all circulant matrices have the same eigenvectors ([23] and p.267 of [24]),

$$u_m = \frac{1}{\sqrt{N}} \{e^{-j2\pi m/N} \cdots e^{-j2\pi (m-1)/N}\},$$

where $[\cdot]^T$ denotes a transpose.

Let $U$ be a matrix consisting of the eigenvectors $u_m$ as columns in order and $\Psi = \text{diag}(\psi_k)$ is the diagonal matrix with diagonal elements $\psi_0, \psi_1, \ldots, \psi_{N-1}$. It is true that $UU^H = U^HU = I_N$, where $I_N$ is an identity matrix and $[\cdot]^H$ denotes transpose and conjugate operation.

**Lemma 1:** ([23] and [24]) Let $C = \{c[(k - n)N]\}$ and $B = \{b[(k - N)N]\}$ be circulant $N \times N$ matrices with eigenvalues $\psi_m$ and $\beta_m$, $m = 0, 1, \ldots, N - 1$, respectively, where

$$\psi_m = \sum_{k=0}^{N-1} c[k] e^{-j2\pi km/N},$$

$$\beta_m = \sum_{k=0}^{N-1} b[k] e^{-j2\pi km/N}.$$
set $A$ has no upper bound. New PGISs can be constructed by applying these properties. In particular, the property 4 of Theorem 4 indicates that applying circular convolution to two arbitrary PGISs generates a new PGIS that cannot be spanned by the two original PGISs. This explains the abundant PGISs available for the proposed scheme.

III. CONSTRUCTION OF DEGREE-4 PGIS OF PERIOD $N=pq$

A. REVIEW STUDY OF DEGREE-4 PGIS CONSTRUCTION

We can make a brief review of degree-4 PGIS construction from [22]. Let $\mathbb{Z}_N$ denote the ring $\{0, 1, \ldots, N - 1\}$ with integer multiplication modulo $N$ and integer addition modulo $N$, and $\mathbb{Z}_N^\times = \mathbb{Z}_N \setminus \{0\}$. First, we would summarize some results of degree-4 PGIS of period $N = pq$ from [22]. Three subsets of $\mathbb{Z}_N^\times$ are defined as follows:

$$S_p = \{np|n = 1, 2, \ldots, q - 1\},$$
$$S_q = \{kq|k = 1, 2, \ldots, p - 1\},$$
and
$$S_1 = \{n|gcd(n, N) = 1, n \in \mathbb{Z}_N^\times\}.$$

Sequence $s = \{s[n]\}_{n=0}^{N-1}$ of period $N = pq$ is defined as

$$s[n] = \begin{cases} a_3, & n = 0, \\ a_0, & n \in S_1, \\ a_1, & n \in S_q, \\ a_2, & n \in S_p. \end{cases}$$

(2)

In [22], three nonlinear equations to govern four coefficients, $a_i = x_i + jy_i, i = 0, 1, 2, 3$, of sequence $s = \{s[n]\}_{n=0}^{N-1}$ to be a degree-4 PGIS are expressed below

$$\begin{align*}
(p - 2)(q - 2)(x_0^2 + y_0^2) + 2(p - 2)(x_0x_2 + y_0y_2) \\
+ 2(p - 2)(x_0x_1 + y_0y_1) \\
+ 2(x_1x_2 + y_1y_2 + x_0x_3 + y_0y_3) = 0,
\end{align*}$$

$$\begin{align*}
(p - 2)(q - 1)(x_0^2 + y_0^2) + (p - 2)(x_1^2 + y_1^2) \\
+ 2(q - 1)(x_0x_2 + y_0y_2) + 2(x_1x_3 + y_1y_3) = 0,
\end{align*}$$

$$\begin{align*}
(q - 2)(x_2^2 + y_2^2) + (p - 2)(q - 2)(x_0^2 + y_0^2) \\
+ 2(p - 1)(x_0x_1 + y_0y_1) + 2(x_2x_3 + y_2y_3) = 0.
\end{align*}$$

(3)

The decomposition method is applied to transform these nonlinear constrained equations of (3) into three linear systems of four equations with $x_2, y_2, x_3, y_3$ as the variables. These linear systems can be expressed using the matrix notation $A_i x = b_i, i = 1, 2, 3$. In these equations, $A_i$ is the coefficient matrix of size $4 \times 4$, $x = [x_2 \ y_2 \ x_3 \ y_3]^T$, and $b_i$ is a data column vector. It has

$$A_2 = \begin{bmatrix} 2(q - 2)x_0 + 2x_1 & 2(q - 2)y_0 + 2y_1 & 2x_0 & 2y_0 \\
2(q - 1)x_0 & 2(q - 1)y_0 & 2x_1 & 2y_1 \\
1 & 1 & 0 & 0 \\
2 - q & q - 2 & -2 & 2 \end{bmatrix},$$

(5)

$$A_3 = \begin{bmatrix} 2(q - 2)x_0 + 2x_1 & 2(q - 2)y_0 + 2y_1 & 2x_0 & 2y_0 \\
2(q - 1)x_0 & 2(q - 1)y_0 & 2x_1 & 2y_1 \\
2 - q & 0 & -2 & 0 \\
0 & 2 - q & 0 & -2 \end{bmatrix},$$

(6)

$$b_1 = [\triangle_1 \ \triangle_2 \ x_0 + y_0 \ (q - 2)(y_0 - x_0) + 2(y_1 - x_1)^2],$$

(7)

$$b_2 = [\triangle_1 \ \triangle_2 \ (q - 2)y_0 + 2y_1 - x_0 \ (q - 2)x_0 + y_0 + 2x_1]^T,$$

(8)

$$b_3 = [\triangle_1 \ \triangle_2 \ (2 - q)x_0 - 2x_1 \ (2 - q)y_0 - 2y_1]^T,$$

(9)

where $\triangle_1 = (2 - p)(q - 2)(x_0^2 + y_0^2) - 2(p - 2)(x_0x_1 + y_0y_1)$ and $\triangle_2 = (2 - p)(q - 1)(x_0^2 + y_0^2) - (p - 2)(x_1^2 + y_1^2)$. By choosing constants $x_0, y_0, x_1, y_1$ such that all $|A_i| \neq 0$, we can always adjust these four constants and derive the integer solutions of four variables $(x_2, y_2, x_3, y_3)$ from equations $x_i = A_i^{-1}b_i, i = 1, 2, 3$. These eight parameters $x_n, y_n, n = 0, 1, 2, 3$, meet the system of three nonlinear equations (3).

B. NEW CONSTRUCTION OF DEGREE-4 PGIS

We can add three new linear systems of four equations to facilitate the cryptographic applications, where the detailed procedures are derived here. The second equation of (3) can be replaced by subtracting from the top equation of (3), after which it becomes

$$\begin{align*}
(x_0 - x_1)((p - 2)(x_0 - x_1) + 2(x_2 - x_3)) \\
+ (y_0 - y_1)((p - 2)(y_0 - y_1) + 2(y_2 - y_3)) = 0.
\end{align*}$$

(10)

The nonlinear equation (10) can be decomposed into two parts, which results in a linear system of two equations. We provide three different decomposition methods, which are respectively presented below

$$\begin{align*}
\begin{cases} x_1 + y_1 = x_0 + y_0, \\
(2 - p)x_1 + (p - 2)y_1 - 2x_3 + 2y_3 \\
= (p - 2)(y_0 - x_0) - 2x_2 + 2y_2. \end{cases}
\end{align*}$$

(11)

$$\begin{align*}
\begin{cases} -x_1 + (p - 2)y_1 + 2y_3 = -x_0 + (p - 2)y_0 + 2y_2, \\
(p - 2)x_1 + y_1 + 2x_3 = (p - 2)x_0 + y_0 + 2x_2. \end{cases}
\end{align*}$$

(12)
Based on the results of (11), (12) and (13), the nonlinear constrained equations of (3) can also be transformed into three linear systems of four equations with \( s \) four variables. These linear systems can be expressed using the matrix notation \( A \mathbf{x} = \mathbf{b} \), where \( A \) is the coefficient matrix of size \( 4 \times 4 \), \( \mathbf{x} = [x_1 \ y_1 \ x_3 \ y_3]^T \), and \( \mathbf{b} \) is a data column vector. It has

\[
A_4 = \begin{bmatrix}
2(p - 2)x_0 + 2x_2 & 2(p - 2)y_0 + 2y_2 & 2x_0 & 2y_0 \\
2(p - 1)x_0 & 2(p - 1)y_0 & 2x_2 & 2y_2 \\
2 - p & p - 2 & -2 & 2 \\
1 & 1 & 0 & 0
\end{bmatrix},
\]

(14)

\[
A_5 = \begin{bmatrix}
2(p - 2)x_0 + 2x_2 & 2(p - 2)y_0 + 2y_2 & 2x_0 & 2y_0 \\
2(p - 1)x_0 & 2(p - 1)y_0 & 2x_2 & 2y_2 \\
-1 & p - 2 & 0 & 2 \\
p - 2 & 1 & 2 & 0
\end{bmatrix},
\]

(15)

\[
A_6 = \begin{bmatrix}
2(p - 2)x_0 + 2x_2 & 2(p - 2)y_0 + 2y_2 & 2x_0 & 2y_0 \\
2(p - 1)x_0 & 2(p - 1)y_0 & 2x_2 & 2y_2 \\
2 - p & 0 & -2 & 0 \\
0 & 2 - p & 0 & -2
\end{bmatrix},
\]

(16)

These linear systems can be transformed into three systems of linear equations in the unknowns \( x_1, y_1, x_3, y_3 \). From equations (3), we derive

\[
x_1 = \begin{bmatrix}
x_0 \\
y_0 \\
x_2 \\
y_2
\end{bmatrix} = (2 - p) \begin{bmatrix} x_0 \\ y_0 \\ x_2 \\ y_2 \end{bmatrix} + \begin{bmatrix} 2x_0 \\ 2y_0 \\ 2x_2 \\ 2y_2 \end{bmatrix} - \begin{bmatrix} 2 \cdot p \\ -p \\ 2 - p \\ p - 2 \end{bmatrix} \mathbf{x}.
\]

Example 2: When \( p = 5 \) and \( q = 7 \), given that \( a_0 = 10j \) and \( a_2 = -10 - 10j \), we derive \( a_1 = 14 - 32j \) from \( A_4 \mathbf{x} = \mathbf{b}_6 \) of (16), where a degree-4 PGIS \( s_{35} \) is of period \( N = 35 \) is given by

\[
s_{35} = \begin{bmatrix}
a_3 \\
a_0 \\
a_0 \\
a_0 \\
a_0 \\
a_0 \\
a_0 \\
a_0 \\
a_0
\end{bmatrix},
\]

(18)

Example 1: When \( p = 5 \) and \( q = 3 \), given that \( a_0 = 6 \) and \( a_1 = -6j \), we derive \( a_2 = -14 + 20j \) and \( a_3 = 25 - j \) from \( A_4 \mathbf{x} = \mathbf{b}_1 \) of (4), where a degree-4 PGIS of period \( N = 15 \) is given by

\[
s_{15} = \begin{bmatrix}
a_3 \\
a_0 \\
a_0 \\
a_0 \\
a_0 \\
a_0 \\
a_0 \\
a_0 \\
a_0
\end{bmatrix}.
\]

(17)

When \( p = 3 \) and \( q = 5 \), we can apply \( A_5 \mathbf{x} = \mathbf{b}_5 \) of (15) to construct PGIS with the same pattern of (17), where \( a_0 = 2 - 4j \) and \( a_2 = 6 - 2j \) are assigned to derive \( a_1 = -8 + 16j \) and \( a_3 = 1 - 17j \).

IV. CIRCULAR CONVOLUTION–TRAPDOOR ONE-WAY PERMUTATION FUNCTION

Let \( y = \{y[n]_{n=0}^{N-1} = \mathbf{x} \otimes s \) denote the circular convolution between \( \mathbf{x} \) and \( s \); that is,

\[
| y[n] = \sum_{\tau=0}^{N-1} s[\tau] \cdot x[(n - \tau)\mod{N}]. 
\]

(19)

The result of \( y = \mathbf{x} \otimes s \) can be expressed using matrix expression

\[
y = \mathbf{X}s,
\]

(20)

where the circulant matrix \( \mathbf{X} \) is given in (21).

When the result of \( y \) in (20) is given, \( s \) can be derived from \( y \) and \( x \) through circular deconvolution, which is equivalent to solving a system of \( N \) linear equations in the \( N \) unknowns \( \{s[n]_{n=0}^{N-1}\} \). The matrix expression of the solution is given by

\[
s = \mathbf{X}^{-1}y.
\]

(22)

In (22), the inverse of a nonsingular \( N \times N \) matrix \( \mathbf{X}^{-1} \) can be computed through Gauss elimination and back-substitution with \( N^3 \) multiplication/division and \( N^3 \) addition/subtractions [25]. With an increase in \( N \), the increasingly heavy computing load can make circular
deconvolution infeasible. However, when \( x \) is a PGIS with energy \( E \), we have \( x \otimes x_1^* = E \cdot \delta_N \). This indicates that the inverse of the coefficient matrix is given by \( X^{-1} = \frac{1}{E} X^H \), and the solution \( s = \frac{1}{E} X^H y \) is obtained directly without a system of \( N \) linear equations being solved.

**Theorem 6:** There exist numerous pairs of non-zero sequences \( x_i \) and \( s_i \) of length \( N \), such that

\[
x_1 \otimes s_1 = x_2 \otimes s_2 = \cdots = x_i \otimes s_i = \cdots
\]

is true; however, \( x_i \neq x_k \Leftrightarrow s_i \neq s_k \).

Proof: Let \( y = \{ y[n] \}_{n=0}^{N-1} \) be a sequence consisting of constants, and \( Y = \{ Y[n] \}_{n=0}^{N-1} \), \( X_i = \{ X_i[n] \}_{n=0}^{N-1} \) and \( S_i = \{ S_i[n] \}_{n=0}^{N-1} \) be the DFTs of \( y \), \( x_i \), and \( s_i \), respectively. Taking the DFT of equations \( y = x_1 \otimes s_1 = x_2 \otimes s_2 = \cdots \), yields

\[
Y = X_1 \circ S_1 = X_2 \circ S_2 = \cdots.
\]

1. To prove \( x_1 \otimes s_2 = x_2 \otimes s_2 = \cdots \) is equivalent to showing that the following solutions exist.

\[
\begin{align*}
Y[0] &= X_1[0]S_1[0] = X_2[0]S_2[0] = \cdots, \\
Y[1] &= X_1[1]S_1[1] = X_2[1]S_2[1] = \cdots, \\
& \vdots \\
Y[N-1] &= X_1[N-1]S_1[N-1] = X_2[N-1]S_2[N-1] = \cdots. \quad (23)
\end{align*}
\]

For any fixed constant \( Y[k] \), there exist numerous pairs of \( (X_i[k], S_i[k]) \), \( i = 0, 1, 2, \ldots \), such that \( Y[k] = X_1[k] \cdot S_1[k] = X_2[k] \cdot S_2[k] = \cdots ; k = 0, 1, 2, \ldots, N - 1 \), is true (i.e., \( 6 = 2 \cdot 3 = (-2) \cdot (-3) = -2 \cdot 3j = \sqrt{6} \cdot \sqrt{6} = \cdot \cdot \cdot \)).

2. Let \( M_i \) and \( M_k \) be two circulant matrices constructed using \( x_i \) and \( x_k \), respectively. The matrix expression of \( y = x_i \otimes s_i \) is given by \( y = M_i S_i \), from which the unique solution \( s_i = M_i^{-1} y \) is derived. Because \( x_i \neq x_k \Leftrightarrow M_i \neq M_k \), \( s_i = M_i^{-1} y \neq s_k = M_k^{-1} y \) is proven.

Theorem 6 indicates that for a given \( y \), numerous pairs of \( (x_i, s_i) \) exist that can satisfy equation \( y = x_i \otimes s_i \); however, when one vector in this pair is given, the other one is uniquely determined. Example 3 presents an example for demonstration. An eavesdropper who hears only the transmitted \( y \) (ciphertext) cannot apply (22) to decrypt \( y \) and obtain \( s \), where the unique solution of equation (22) is evaluated on the basis of the assumption that \( y \) and \( x \) are available.

In contrast to the factorization of a product of two prime numbers featuring one-to-one mapping between a pair of two primes \( (p, q) \) and \( N (= pq) \), circular convolution features multiple-to-one mapping among a pair of two sequences \( (x_i, s_i) \) and the resultant \( y = x_i \otimes s_i \). The multiple-to-one mapping property of circular convolution complicate or even prevents the operation of circular deconvolution, and is thus considered one-way. When \( x_i \) is available and is a PGIS, the operation of circular deconvolution becomes straightforward, with PGIS \( x_i \) acting as the trapdoor for circular convolution. In addition, circular convolution is commutative, with \( x_i \otimes s_i = s_i \otimes x_i \). The circular convolution operation over PGISs is trapdoor one-way permutation.

**Example 3:** Let \( \{ s_i \}_{i=0}^5 \) be six sequences of period 13. These sequences are given by

\[
\begin{align*}
s_0 &= (-9 - 3j, -9 - 3j, 4 + 23j, -9 - 3j, 4 + 23j), \\
s_1 &= \frac{1}{835} (-55 - 25j, -107 + 79j, 23 - 181j), \\
s_2 &= \frac{9}{835} (-1 - 43j, 12 - 69j, -14 - 17j, -40 + 35j, 12 - 69j, -53 + 61j, -27 + 9j, -27 + 9j, -14 - 17j, -40 + 35j, -27 + 9j, -14 - 17j), \\
s_3 &= (0, 0, 1, 0, 1, 1, 1, -1, -1, 0, 1, -1, 1), \\
s_4 &= (2, -2, 8, -3, -2, 1, -7, 5, 5, 6, 2, 9, 3), \\
s_5 &= (a, b, b, b, b, b, b, b, b, b, b, b, b),
\end{align*}
\]

where \( a = 10 + 25j \), and \( b = -3 - j \).

Thus, \( s_0 \otimes s_1 = s_2 \otimes s_2 = s_3 \otimes s_4 \) can easily be verified, where

\[
s_0 \otimes s_1 = (18, 27, 9, -9, 27, -18, 0, 9, -9, 0, 9, 18).
\]

**V. PGIS-BASED HYBRID PUBLIC/PRIVATE KEY CRYPTOGRAPHY**

**A. CIPHER ENCRYPTION AND DECRYPTION SCHEME**

As described in [2], the encryption and decryption procedures typically consist of a general method and an encryption key. RSA uses exponentiation modulo a product of two very large primes for data encryption and decryption. Its security is connected to the extreme difficulty of factoring large integers. The encryption key is the pair of positive integers \( (e, n) \), and the private decryption key is another pair of positive integers \( (d, n) \).

In our proposed cipher encryption and decryption scheme, the \( N \)-point circular convolution and a set of PGISs of period \( N = pq \) can function as the general method and the encryption key, respectively. The public key is \( (N, x_0, y_0, x_1, y_1, A_i, b_i) \). In section III, four coefficients \( x_i + jy_i, i = 0, 1, 2, 3 \) for constructing a degree-4 PGIS are governed by a system of four linear equations \( A_i x = b_i \), from which \( x = A_i^{-1} b_i \) can be derived. The associated degree-4 PGIS \( s \) constructed using this set of four coefficients \( x_i + jy_i \) can serve as the encryption sequence to generate ciphertext by circularly convoluting it with block data plaintext of size \( N \). Because the elements of \( x = [x_2 y_2 x_3 y_3]^T = A_i^{-1} b_i \) are uniquely determined by six values of \( x_0, y_0, x_1, y_1, p \), and \( q \), the decryption sequence \( s_{N-1} \) can easily be generated by an authorized user with the assigned public key \( (N, x_0, y_0, x_1, y_1, A_i, b_i) \) and private key number \( p \) or \( q \). However, to malicious cryptanalysts, the
public key cannot generate the decryption sequence without the actual value of \( p \) or \( q \). When both \( p \) and \( q \) are long strong primes, the difficulty of factoring \( N \) into \( p \) and \( q \) provides the same security level as that of the RSA scheme.

Let \( A = \{s_1, s_2, \ldots, s_n\} \) be a set of PGISs of period \( N \), where there is no upper bound for the cardinality \( n \) of set \( A \). A private sequence \( s \) with energy \( E \) is randomly chosen from set \( A \) to serve as the encryption sequence. Let \( m = \{m[n]\}_{n=0}^{M-1} \) denote the input plaintext of length \( M \), where \( M = kN \). We express \( m = \{m_1, m_2, \ldots, m_k\} \). If \( M \) cannot be divided by \( N \), we can insert additional zeros at the end of \( m \) to make it true. However, when \( M < N \), we should insert additional \( N - M \) zeros to form the plaintext.

The plaintext \( m_i \) is circularly convoluted with the encryption key \( s \) to generate the ciphertext \( c_i = s \otimes m_i \). Note that the encryption key associated with user \( B \) should properly be subscribed as \( s_B \), because each user has a private key sequence. However, we consider only a typical case, and the subscript is omitted.

The detailed procedures for encryption using PGIS \( s \) and decryption using \( s_{-1}^* \) are summarized as follows:
1. At the transmitter end, circular convolution between the encryption key \( s \) and \( m_i \) generates the ciphertext
   \[
   c_i = s \otimes m_i, \quad i = 1, 2, \ldots, k.
   \]
2. The ciphertext \( c = (c_1, c_2, \ldots, c_k) \) and public key \((N, x_0, y_0, x_1, y_1, A_i, b_i)\) are transmitted through the common channel. The private key \( p \) can be shared by the Diffie-Hellman key exchange algorithm [3].
3. At the receiver end, after the receipt of \( c_i \), only the intended receiver who holds the private key \( p \) can generate the decryption sequence \( s_{-1}^* \), and the original plaintext can be decrypted using circular convolution between \( c_i \) and \( s_{-1}^* \): that is,
   \[
   \frac{1}{E} c_i \otimes s_{-1}^* = \frac{1}{E} (m_i \otimes s \otimes s_{-1}^*) = \frac{1}{E} (m_i \otimes E \cdot \delta_N) = m_i, \quad i = 1, 2, \ldots, k.
   \]

To demonstrate the proposed scheme, let \( m_i = (1, -1, 1, 1, -1, 1, 1, 1, -1, 1, 1, 1, -1) \) be the binary plaintext of length \( N = 15 \). We can define four base sequences \( e_i \), \( i = 0, 1, 2, \) and \( 3 \) as follows, to construct a degree-4 encryption PGIS \( s \) of period \( N = p \cdot q = 5 \cdot 3 = 15 \).

\[
\begin{align*}
e_0 &= (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1), \\
e_1 &= (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0), \\
e_2 &= (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0), \\
e_3 &= (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0).
\end{align*}
\]

Let \( a_1 = x_i + jy_i \) be four coefficients. By inputting \( x_0 = 24, y_0 = 0, x_1 = 0, y_1 = -24, p = 5 \), and \( q = 3 \) into \( A_1 \) and \( b_1 \) in equations (4) and (7), we derive \( x_2 = -56, y_2 = 80, x_3 = 100, \) and \( y_3 = -4 \). A degree-4 PGIS \( s \) is given by
   \[
   s = a_0 e_0 + a_1 e_1 + a_2 e_2 + a_3 e_3 = (25 - j, 6, 6, -6j, 6, -14 + 20j, 6, -6j, 6, 6),
   \]

**Example 4:** The ciphertext \( c_i = m_i \otimes s \) is given by

\[
\begin{align*}
c_i &= s \otimes m_i = (25 - 25j, -29 + 41j, 9 + 39j, 25 - 25j, 11 + j, 49 - j, 25 - 25j, 21 + 51j, -41 + 29j, 65 - 65j, -29 + 41j, 49 - j, -15 + 15j, 61 + 11j, -1 - 11j) \quad (25)
\end{align*}
\]

The ciphertext \( c_i \) in (25) and public key \((15, 24, 0, 0, -24)\) are transmitted through a common channel to the receiver. At the receiver end, the original plaintext \( m_i \) can be recovered from taking circular convolution between \( s_{-1}^* \) and \( \hat{c}_i \) which is the estimation of \( c_i \). It has

\[
\begin{align*}
\hat{m}_i &= \frac{1}{2500}(\hat{c}_i \otimes s_{-1}^*) \\
&= (1, -1, 1, 1, -1, 1, 1, 1, -1, 1, 1, 1, -1) + n, \quad (26)
\end{align*}
\]

where the energy of encryption sequence \( s \) is 2250, and \( n \) denotes the received white noise vector. When the signal-to-noise ratio is sufficiently high, the estimation of \( m_i \) from \( \hat{m}_i \) (\( \hat{m}_i \rightarrow m_i \)) is straightforward. However, when the received ciphertext \( \hat{c}_i \) is decrypted using the conjugate of encryption sequence \( x_1 = s^* \) instead of \( s \), the resultant \( m_{1i} \) is expressed as follows:

\[
\begin{align*}
m_{1i} &= \hat{c}_i \otimes x_{-1}^* = c_i \otimes s_{-1}^* + n_i = \frac{1}{1125}(1100 - 25j, -1084 + 29j, 1164 - 9j, 1100 - 25j, -1124 - 11j, 1124 - 49j, 1100 - 25j, 1176 - 21j, -1096 + 41j, 1060 - 65j, -1084 + 29j, 1124 - 49j, 1140 + 15j, 1136 - 61j, -1136 + j) + n_i, \quad (27)
\end{align*}
\]

We found that although similarity exists between \( s \) and \( x_1 = s^* \), the contents of \( \hat{m}_i \) and \( m_{1i} \) are extremely different. The plaintext \( m_i \) can be estimated from \( \hat{m}_i \), but \( m_{1i} \) is unlikely to be derived from \( m_{1i} \). **Example 4** demonstrates that effective decryption can only be carried out through the unique private key sequence \( s \).

### B. Efficient Scheme for Processing Digital Signatures

Let \( b = \{b[n]\}_{n=0}^{N-1} \) be a nonzero sequence of length \( N \), in which \( b[n] \in \{1, 0\} \) is preferable to lighten the computing load. We can apply an additional private encryption sequence \( s_b \) to generate sequence \( d = s_b \otimes b \). \( d \) and \( b \) can be attached to ciphertext \( c = (c_1, c_2, \ldots, c_k) \) as the overhead of the document; that is, the transmitted ciphertext becomes \((d, b, c_1, c_2, \ldots, c_k)\). After the receipt and detection of \( d \) and \( b \), the receiver performs an authentication check to verify the origination of the consecutive ciphertext by examining whether the condition \( S_b^T b = d \) holds, where \( S_b \) is the circulant matrix constructed using encryption sequence \( s_b \). The pair of two sequences \((d, b)\) can serve
as efficient digital signatures for the associated PGIS-based cipher encryption scheme because a pair of $(d, b)$ cannot be forged. In addition, a signer cannot later deny the validity of his or her signature because $d = s_b \otimes b$ is uniquely determined by a private key $s_b$. To operate digital signatures simultaneously with cipher encryption, the public key becomes $(N, x_0, y_0, x_1, y_1, x_{0b}, y_{0b}, x_{1b}, y_{1b}, A_i, B_i)$, where the additional four coefficients $x_{0b}, y_{0b}, x_{1b},$ and $y_{1b}$ are assigned for generating $s_b$ by authorized users.

VI. COMPARISON OF PROPOSED SCHEME WITH OTHER CRYPTOSYSTEMS

The proposed scheme is considered a form of hybrid public/private key cryptography, and the comparison of public, private and the proposed key cryptography is addressed in this section. Public-key cryptography has two primary use cases: authentication and confidentiality, which messages can be signed with a private key, and then anyone with the public key is able to verify that the message is created by someone possessing the corresponding private key. Without authentication, it is easy for attackers to modify the message, and in many flawed systems even decrypt messages. However, most public-key encryption schemes can only encrypt small chunks of data at a time, much smaller than the messages we want to be able to send. Public-key schemes are also generally quite slow, much slower than their private key counterparts. By contrast, private-key cryptography encounters private key distribution and management problem. The number of key exchanges grows about as fast as the number of people squared. The fundamental problem of large number of key exchanges has not been solved yet. The computing load of the proposed scheme, which circular convolution is applied to encrypt and decrypt a message, is smaller than the other two schemes. However, this scheme still relies on key exchange algorithm to share a common secret key number. The proposed scheme might take the advantages of the other two schemes, which can make a balance between two extremes. We make the more detailed comparisons in the following two subsections.

A. COMPARISON BETWEEN RSA AND PROPOSED SCHEME

RSA and the proposed scheme based on PGISs are compared as follows:

1) Data encryption using exponentiation modulo $N$ ($c = m^e \mod N$) does not increase the size of a message. This is the merit of the RSA scheme. However, when plaintext is circularly convoluted with a PGIS that has large coefficients, the ciphertext also contains larger values. In addition, the energy level of ciphertext is proportional to the period of the PGIS, which should be sufficiently large to provide the desired security. The escalation of the energy level poses a major challenge to the implementation and transmission of the resultant ciphertext. This topic is further addressed in Section VII.

2) The public-key cryptosystem based on the RSA scheme provides an effective method for key management and authentication, but it is inefficient for the bulk encryption of data. In addition, to apply the RSA scheme for data encryption, the message can only be an integer in the interval $[0, N - 1]$; however, there is no such data type restriction when data encryption is conducted through circular convolution operation. Therefore, the proposed scheme has more potential applications.

3) The capacity ($C$) of a cryptosystem is defined as the maximum number of authorized users the associated system can support simultaneously. Consider either a multiple-to-one or a multiple-to-multiple secure communication scenario, where the capacity of a cryptosystem based on the RSA scheme is determined by the number of available pairs of exponents $(d, e)$, because each pair of two parties should have a unique $(d, e)$ key pair. For each $N_i = p_i q_i$, the number of pairs of private key $d_i$ and public key $e_i$, which satisfies $d_i e_i \equiv 1 \mod (p_i - 1)(q_i - 1)$, cannot compete the unbounded cardinality of a set of PGISs of period $N_i$ by Theorem 5. Actually, it is imperative for each pair of two parties to choose its own RSA modulo $N_i$ to avoid common modulus attack. When many pairs of $(e_i, d_i)$ are assigned associated with the same $N_i$, knowledge of any $(e_i, d_i)$ pair allows for the factorization of the modulus $N_i$, and hence any entity could subsequently determine the decryption exponents of all other entities in the network. Also, if a single message were encrypted and sent to two or more entities in the network, then there is a technique by which an eavesdropper (any entity not in the network) could recover the message with high probability using only publicly available information [26]. However, the proposed PGIS-based scheme using circular convolution for data encryption will not encounter the common modulus attack problem.

4) To meet future high demand for secure communications over public networks, the values of $N_i = p_i q_i$ must be allowed to escalate without an upper bound to achieve high system capacity requirement when a cryptosystem is operated based on the RSA scheme. When $N_i$ is extremely large, it becomes unrealistic to use the exponentiation modulo $N_i$ algorithm to implement data encryption because of excessive time complexity. Therefore, a PGIS-based cryptosystem is preferred because the abundant PGISs are available for a fixed $N_i$, although implementing such a system requires more memory and bandwidth.

B. COMPARISON BETWEEN PRIVATE-KEY AND PROPOSED SCHEME

To most private-key cryptography, the operation of data encryption between private key and message is based on element-wise operation. We can take one-time pad scheme as an example, where the XOR operation between two binary streams is made in a bit-by-bit manner, which is a special case of element-by-element manner. Circular convolution of two sequences produces one sequence of the same period, where value of the $n$th entry $y[n] = \sum s[\tau] \cdot x[(n - \tau)N], \text{defined in}$
is the inner product of two sequences (vectors) \( s \) and the 
non steps circular shift of \( x \), denoted by \( x^{(n)} \), is obtained from processing two sets of data, 
which are two vectors, rather than two data elements. 
Let sequence \( s = \{s[n]\}_{n=0}^{N-1} \), where \( s[n] = s_n \). This implies 
\[
\mathbf{s} = \mathbf{s}_0 \cdot \mathbf{\delta}_N + s_1 \cdot \mathbf{\delta}_N^{(1)} + \cdots + s_{N-1} \cdot \mathbf{\delta}_N^{(N-1)},
\]
where \( \mathbf{\delta}_N^{(n)} \) denotes the circular shift of \( \mathbf{\delta}_N \) to the right by \( n \) 
steps. Based on the fact that \( \mathbf{m} \otimes \mathbf{\delta}_N^{(n)} = \mathbf{m}^{(n)} \), we can express 
circular convolution between \( \mathbf{m} \) and \( \mathbf{s} \) as follows: 
\[
\mathbf{m} \otimes \mathbf{s} = \mathbf{s}_0 \cdot \mathbf{m} + s_1 \cdot \mathbf{m}^{(1)} + \cdots + s_{N-1} \cdot \mathbf{m}^{(N-1)}.
\] (28)

Private-key cryptography and the proposed scheme based on 
PGISs are compared as follows:

1. Equation (28) implies that circular convolution between 
\( \mathbf{m} \) and \( \mathbf{s} \) is a linear combination of \( \mathbf{m} \) and its 
circular shifts, which linear combination is obvious a vector-wise 
operation, and the coefficients of linear combination and 
the number of circular shifts are determined by the number of 
nonzero elements of \( \mathbf{s} \). The vector-wise operation is more 
complex than the element-wise operation, but the former one 
has more potential to achieve confidential capacity to the 
proposed cryptosystem. The reason is that the combination 
of individual parts into single one is straightforward; however, 
the inverse operation of decomposition the resultant output 
into individual parts is difficult.

2. Different inner product of two vectors can result in the 
same scalar output, and this is the reason circular convolu-
tion features multiple-to-one mapping between different 
pairs of sequence set \( \{ (x_i, s_i) \} \) and the resultant output 
\( y = x_1 \otimes s_1 = \cdots = x_i \otimes s_i = \cdots \). Without the PGIS 
key, an eavesdropper trying to extract information from a set of 
ciphertexts is difficult, especially when the period \( N = pq \) 
of the PGIS key is large enough, where the computing load 
of solving multiple-to-one mapping problem is formidable.

3. Private key can only be used one time to the one-time 
pad scheme, and to other private-key cryptosystem such as 
DES and AES, reusing private key is still not suggested 
from confidentiality point of view, especially because it is 
an element-wise operation. Thus, to communicate between 
\( n \) users in a public network, it needs \( \frac{n(n-1)}{2} \) key exchanges, 
which the number of key exchanges grows about as fast as 
the number of people squared. The vector-wise operation 
of the proposed scheme contributes not only confidentiality 
but also the applicability of reusing the same PGIS key in 
a public network. As shown in Section VIII, operating linear 
combination to message and its circular shifts can contribute 
larger differences to the resultant ciphertext, even though 
messages have smaller differences between each other.

VII. ANALYSIS OF APPROXIMATION ERROR

Let \( A = \{s_1, s_2, \ldots, s_m\} \) be a set of PGISs. The cardinality 
\( m \) of \( A \) can be as large as needed, depending on the capacity 
requirement of the cryptosystem. When more PGISs of the 
same pattern are constructed from the solutions of the same 
constraint equations, the values of the resultant coefficients 
gradually increase. Therefore, energy levels of these PGISs 
escalate. When plaintext is circularly convoluted with a PGIS 
that belongs to a higher energy level, the energy of the 
associated ciphertexts escalates beyond that of the ciphertexts 
convoluted with PGISs that contain smaller coefficients.

Differing ciphertext energy levels might provide a method 
for adversaries to sift through PGISs and initiate a ciphertext 
attack. To overcome this problem and reduce the number 
of digits required to represent the resultant ciphertext, all 
PGISs in the same set should be normalized to the same 
unit energy. In this case, the energy level of a ciphertext can 
remain the same as that of the original plaintext; thus, all 
ciphertexts have the same energy level. However, when the 
square root energy \( \sqrt{E} \) of a PGIS is an irrational number, 
the coefficients of the normalized PGIS become irrational as 
well. This presents a considerable challenge for the imple-
mentation and transmission of the resultant ciphertexts, given 
that an infinite number of digits are required to represent 
an irrational number. In this section, the performance of 
the proposed encryption scheme is analyzed when the irrational 
coefficients of the normalized PGISs are stored and processed 
using a finite number of digits.

A. MODEL OF APPROXIMATION ERROR

Let \( s_{ai} = s + e_{ai} \) be the approximation of \( s \) performed 
containing the first \( i \) digits of an irrational number, where 
\( e_{ai} \) is the approximation error. Given that all sequences 
are normalized with the unit energy, the values of all coeffi-
cients of the sequences are less than one, except for those 
of the degree-1 PGIS. Let \( \pm d_1 d_2 \cdots d_i \cdots \) be a typical 
irrational coefficient, where the value of the \( i^{th} \) digit \( d_i \in \{0, 1, \ldots, 9\} \). We apply the following algorithm to operate 
the irrational number approximation:

\[
d_i = \begin{cases} 
  d_i, & \text{when } d_{i+1} \in \{0, 1, \ldots, 4\} \\
  d_i + 1, & \text{when } d_{i+1} \in \{5, 6, \ldots, 9\}.
\end{cases}
\] (29)

When \( d_{i+1} \in \{0, 1, \ldots, 4\} \), we can preserve the former \( i \) 
digits untouched to finish the approximation, which yields 
\( \pm d_1 d_2 \cdots d_i \). For \( d_{i+1} \in \{5, 6, \ldots, 9\} \), when adding “1” to 
the original \( i^{th} \) digit does not cause overflow, the former \( i-1 \) 
digits are maintained and \( d_i \) is substituted with \( d_i + 1 \) to yield 
\( \pm d_1 d_2 \cdots d_{i-1} (d_i + 1) \). When adding “1” to the original 
\( i^{th} \) digit causes overflow, \( d_i = 0 \) and \( d_{i-1} = d_{i-1} + 1 \) are 
assigned, and overflow checking moves backward one digit 
to the resultant \( d_{i-1} + 1 \). This process should be performed 
backward one digit at a time until the overflow stops. 
The resultant approximation becomes \( \pm d_1 d_2 \cdots d_{i-1} (d_i + 1) \) 
where \( 1 \leq r < i \) is the entry where the overflow stops.

The approximation error caused by using only \( i \) digits to 
represent an irrational number is similar to that of quanti-

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/
The quantization noise caused by using finite quantization levels to approximate an analog signal in a digital signal processing unit. The quantization noise is modeled to be uniformly distributed within the interval $[-\Delta/2, \Delta/2]$ and $\Delta$ is the quantization step. When the overflow problem is ignored, the approximation error in each entry of $e_i$, is located within the interval $[-10^{k-1}, 10^{k-1}]$; thus, it can be modeled to be uniformly distributed within this interval as quantization noise. Given that the variance of the uniform distribution is $\Delta^2/12$, and the size of an approximation error vector is $N \times 1$, the overall variance of the approximation error is $N \cdot 10^{-2k}/12$. When the error-to-signal power ratio is defined as $\frac{E_a}{S} = \frac{|a_i - s_i|^2}{\sigma^2}$, where $|s|^2 = 1$, the ratio is given by

$$E_a \over S = -20i - 10 \log 12 + 10 \log N \text{ dB.}$$  \hspace{1cm} (30)$$

Equation (30) indicates that a low error-to-signal power ratio $\frac{E_a}{S}$ can be achieved when more digits are used to approximate an irrational number; however, processing and transmitting the resultant ciphertexts requires additional memory and bandwidth. In addition, the large period $N$ of an encryption key escalates the error-to-signal ratio. Fig. 1 compares the $\frac{E_a}{S}$ of four periods ($N = 10^4, 10^6, 10^8$, and $10^9$), when the number of digits varies from three to nine. This figure shows that the $\frac{E_a}{S}$ power ratio can reach to $-50$ dB level, when there are four, five, and six digits for the periods of $N = 10^4, 10^6$, and $10^8$, respectively; and the $\frac{E_a}{S}$ power ratio decreases by $-20$ dB when one more digit is used for approximation.

Fig. 2 presents the number of digits required to achieve the desired $\frac{E_a}{S}$ levels of $-35, -45, -55,$ and $-65$ dB, respectively, when the period of the PGIS is in the interval between $10^5$ and $10^9$. If the threshold of $\frac{E_a}{S}$ power ratio is set at $-45$ dB level, four to six digits are required to represent an irrational number, five to seven digits are required to meet $-55$ dB threshold, and so on. We can summarize the relationship among $\frac{E_a}{S}$, the period of PGIS, and the number of digits as follows:

1) When the period of the PGIS is fixed, the addition of one more digit to approximate an irrational number contributes a gain of $20$ dB to the $\frac{E_a}{S}$ power ratio; thus, an inverse relationship exists between $\frac{E_a}{S}$ and the number of digits.

2) When the required $\frac{E_a}{S}$ power ratio is set as the threshold, the period of the PGIS is proportional to the number of digits required to achieve the desired $\frac{E_a}{S}$ level; more digits are required when the period of PGIS is increased.

**B. SIMULATION EXAMPLES**

In this section, $s$ denotes the normalized original PGIS $s$; however, we retain the four coefficients $a_k$, $k = 0, 1, 2,$ and $3$ of PGIS for simplicity. Let $a_{ik}$ denote the approximation of $a_k$ performed using the first $i$ digits. For period $N = pq$, the numbers of $a_k$ that appear in the PGIS are $(p-1)(q-1)$, $p-1$, $q-1$, and $1$; thus, the actual approximation power error should be $\frac{E_a}{S} = -(p-1)(q-1) \cdot |a_{01} - a_0|^2 + (p-1) \cdot |a_{11} - a_1|^2 + (q-1) \cdot |a_{21} - a_2|^2 + |a_{31} - a_3|^2$. The theoretical error-to-signal power ratio of equation (30), which is $\frac{E_a}{S} = -20i - 10 \log 12 + 10 \log N \text{ dB}$, provides a mathematical estimation of the approximation error. We present two extreme examples to demonstrate the results of approximation, where the coefficients of one PGIS are relatively small compared with the other one, and the period of PGIS is $N = 3 \cdot 5$, where $p = 3$ and $q = 5$. The four coefficients of the first PGIS are $a_0 = 20 - 10j$, $a_1 = 10j$, $a_2 = 8 + 2j$, and $a_3 = -135 - 161j$, and the PGIS is
normalized to be
\[ \bar{s}_s = \frac{1}{3\sqrt{5402}} (a_3, a_0, a_0, a_0, a_1, a_2, a_0, a_0, a_2, a_1, a_0, a_2, a_0, a_0, a_1, a_2, a_0, a_0, a_2, a_0, a_0, a_0). \] (31)

To the second PGIS, each coefficient consists of ten digits, which \( b_0 = -1933763400 - 1659254400j, b_1 = -133594380 + 183006000j, b_2 = -1791601386 + 1432299606j, \) and \( b_3 = 4630497750 + 152422992j. \) The normalized PGIS is given by
\[ \bar{s}_l = \frac{1}{\sqrt{E_l}} (b_3, b_0, b_0, b_2, b_0, b_1, b_2, b_0, b_0, b_2, b_1, b_0, b_2, b_0, b_0), \] (32)
where the energy \( E_l \) of \( \bar{s}_l \) is \( E_l \approx 4.313209552479988 \times 10^{19}, \) requiring 20 digits to represent the actual value of \( E_l. \)

Let \( \bar{s}_{sk} \) and \( \bar{s}_{lk} \) be the approximations of \( \bar{s}_s \) and \( \bar{s}_l \) obtained using the first \( k \) digits. \( e_{sk} = \bar{s}_s - \bar{s}_{sk} \) and \( e_{lk} = \bar{s}_l - \bar{s}_{lk} \) denote the approximation errors. The powers of approximation error \( |\bar{s}_s - \bar{s}_{sk}|^2 \) obtained using the first three to six digits of \( \bar{s}_s \) are \(-56.2439, -75.2597, -95.2683, \) and \(-114.6637 \) dB, respectively; whereas for the second \( \bar{s}_l \), these values become \(-55.7636, -74.7238, -93.9428, \) and \(-114.9137 \) dB, respectively. These two examples demonstrate that the power levels of the approximation errors of two normalized PGISs are basically the same, regardless of the difference between their original coefficients. Even the worst case, which is \(-55.7636 \) dB, is still relatively small compared with general noise, in which only three digits are used for approximation.

The period \( N = 15 \) of the preceding examples is rather small, deviating from the longer period required for the proposed scheme to achieve the desired security. However, we can explain that as the period \( N \) increases from 15 to \( 15 \times 10^{10}, \) although the coefficients differ in order for the associated sequence to be a PGIS, the relative power of the error escalates from approximately \( 10\log 15 \) dB to \( 10\log (15 \times 10^{10}) \) dB, incurring an additional power loss of \( 10 \cdot \log (10^{10}) = 100 \) dB. We can apply five more digits for irrational coefficient approximation to compensate for this additional power loss, because the inclusion of one more digit to approximate the irrational coefficients contributes a 20 dB power gain.

Let \( \mathbf{m} = (1, -1, -1, 1, 1, 1, -1, 1, -1, 1, -1, 1, -1, 1) \) be the message. Ciphertext \( \mathbf{c}_s = \mathbf{m} \otimes \bar{s}_s \) and \( \mathbf{c}_l = \mathbf{m} \otimes \bar{s}_l \) denote the exact ciphertext generated using the exact normalized \( \bar{s}_s \) and \( \bar{s}_l \), respectively, and those generated using the approximations are denoted by \( \mathbf{c}_{s\bar{s}} \) and \( \mathbf{c}_{l\bar{s}}, \) respectively. The results are expressed as follows:

\[
\mathbf{c}_s = \mathbf{m} \otimes \bar{s}_s \\
= \frac{1}{3\sqrt{5402}} (-159 - 137j, 215 + 101j, 135 + 181j, \ldots)
\] (33)

\[
\mathbf{c}_{s\bar{s}} = \mathbf{m} \otimes \bar{s}_{s\bar{s}} \\
\approx (-0.722 - 0.622j, 0.976 + 0.46j, 0.612 + 0.82j, \ldots)
\]

\[
\mathbf{c}_{l\bar{s}} = \mathbf{m} \otimes \bar{s}_{l\bar{s}} \\
\approx (0.217 + 0.509j, -0.781 - 0.179j, -0.745 + 0.033j, \ldots)
\]

We ignore noise contamination to simplify the analysis and comparison of performance using finite numbers of digits. At the receiver end, the authorized receiver can apply the exact encryption sequence \( \mathbf{s}_{s\bar{s}l} \) to decrypt the transmitted approximation ciphertexts \( \mathbf{c}_{s\bar{s}} \) and \( \mathbf{c}_{l\bar{s}} \) because the public key can consist of original coefficients instead of the normalized coefficients. We present only the results of \( \mathbf{m}_{s\bar{s}} \) and \( \mathbf{m}_{l\bar{s}} \) for demonstration.

\[
\mathbf{m}_{s\bar{s}} = \frac{1}{\sqrt{E_l}} \mathbf{s}_{s\bar{s}} \otimes \mathbf{c}_{s\bar{s}} \\
\approx (-1.0012 + 0.0003j, -1.0018 - 0.0008j, -0.9992 + 0.0003j, 0.9996 + 0.0001j, \ldots)
\]

\[
\mathbf{m}_{l\bar{s}} = \frac{1}{\sqrt{E_l}} \mathbf{s}_{l\bar{s}} \otimes \mathbf{c}_{l\bar{s}} \\
\approx (1.0012 + 0.0003j, 1.0018 - 0.0008j, 0.9992 - 0.0003j, 0.0001j, \ldots)
\]

The plaintext \( \mathbf{m} \) can be derived from \( \mathbf{m}_{s\bar{s}} \) in (35) through estimation as follows:

\[
\mathbf{m}_{s\bar{s}} \rightarrow (1, -1, -1, 1, 1, 1, -1, 1, -1, 1, -1, 1, -1, 1, -1, 1, -1, 1).
\]

We have

\[
\mathbf{m}_{l\bar{s}} = \frac{1}{\sqrt{E_l}} \mathbf{s}_{l\bar{s}} \otimes \mathbf{c}_{l\bar{s}} \\
\approx (0.9995 + 0.0014j, -0.9997 - 0.0007j, 0.0001j, \ldots)
\]

\[
\mathbf{m}_{l\bar{s}} \rightarrow (1, -1, -1, 1, 1, 1, -1, 1, -1, 1, -1, 1, -1, 1, -1, 1, -1, 1, -1, 1).
\] (36)
which

\[ \mathbf{m}_{13} \rightarrow (1, -1, -1, 1, 1, -1, 1, -1, 1, -1, 1, -1, 1, -1, 1). \]

To evaluate the overall errors caused from the coefficients approximation of a normalized PGIS, we have

\[ \mathbf{m}_{sk} = \frac{1}{\sqrt{E}} \mathbf{c}_{sk} \otimes \mathbf{s}^{-1} = \frac{1}{\sqrt{E}} \mathbf{m} \otimes (\mathbf{s} - \mathbf{e}_{sk}) \otimes \mathbf{s}^{-1} \]

\[ = \mathbf{m} - \frac{1}{\sqrt{E}} \mathbf{m} \otimes \mathbf{e}_{sk} \otimes \mathbf{s}^{-1}, \]

(37)

and

\[ \mathbf{c}_{sk} = \mathbf{m} \otimes \mathbf{s}_{sk} = \mathbf{c}_{s} - \mathbf{m} \otimes \mathbf{e}_{sk}, \]

(38)

The equations (37) and (38) implies that

\[ |\mathbf{m} - \mathbf{m}_{sk}|^2 = \frac{1}{E} |\mathbf{m} \otimes \mathbf{e}_{sk} \otimes \mathbf{s}^{-1}|^2 = |\mathbf{m} \otimes \mathbf{e}_{sk}|^2 \]

\[ = |\mathbf{c}_{s} - \mathbf{c}_{sk}|^2, \]

(39)

where \( \frac{1}{E}|\mathbf{s}|^2 = \frac{1}{E}|\mathbf{s}^{-1}|^2 = 1. \)

We conclude that

\[ \frac{|\mathbf{m}_{sk} - \mathbf{m}|^2}{|\mathbf{m}|^2} = |\mathbf{e}_{sk}|^2 = |\mathbf{s}_{s} - \mathbf{s}_{sk}|^2. \]

(40)

The equation (40) demonstrates that the power of the error-to-signal ratio of the proposed cipher encryption is solely determined by the approximation error, without calculation of the noise contamination. When \( k \) digits are used to approximate the normalized encryption key sequence, the memory space and transmission bandwidth of the ciphertext are \( 2k \) times that of plaintext because a complex coefficient has the real and the imaginary two parts.

VIII. ADAPTATION TO IOT APPLICATIONS

With the fast development of IoT, the usage of various smart applications such as smart home, smart traffic, and smart cities are increased exponentially. However, the encryption sequence \( \mathbf{s} \) that can be generated by an authorized user with the assigned public key \((N, x_0, y_0, x_1, y_1, A_i, b_i)\) and private key \( p \) or \( q \) might not be realized at the node of IoT devices due to the resource constraints (low computation power and less memory). Lightweight solution is the required unique security feature for IoT platform. Theorem 7 provides a theoretical mean to adapt the proposed scheme for IoT applications, where the computing load of constructing the encryption PGIS key at the IoT devices can be released.

Let \( \mathbf{w} = \{w[n]\}_{n=0}^{N-1} \) be a GIS of odd prime period \( N = p \). In addition, let a new GIS \( \mathbf{w}' = \{w'[n]\}_{n=0}^{mN-1} \) of period \( m \cdot N \) be constructed by upsampling \( \mathbf{w} \), that is,

\[ w'[n] = \begin{cases} w\left[\frac{n}{m}\right], & n = 0, m, \ldots, (N-1)m \\ 0, & \text{otherwise} \end{cases} \]

(41)

**Theorem 7:** (10) Let \( \mathbf{w} = \{w[n]\}_{n=0}^{N-1} \) be a GIS of finite degree. The upsampled \( \mathbf{w}' \) in (41) is also a PGIS with the same degree.

To operate the proposed scheme at the IoT platform, PGIS \( \mathbf{w} \) of prime period \( N = p \) can be implanted at the IoT devices in advance, where the prime number \( p \) might not be large. PGIS \( \mathbf{w} \) should be kept secret, and we can update \( \mathbf{w} \) when it is necessary. Given that PGIS \( \mathbf{w} \) is available, the upsampled PGIS \( \mathbf{w}' \) becomes the encryption private key to create ciphertext, where the upsampling factor \( m \) is determined by the size of plaintext. The receiver end can apply \( \mathbf{w}'_{-1} \) to decrypt the ciphertext. The modified version of proposed scheme is characterized by lower computing load because the upsampled \( \mathbf{w}' \) is a sparse PGIS, where \((m-1)p\) coefficients of \( \mathbf{w}' \) are zeros.

Let "temperature is twenty degrees now" be the message. This message consists of 33 units, which are 29 letters and four empty space. We would like inserting two zeros at the end of message to make it a composite number \( 35 = 5 \times 7 \). When 26 letters in the English alphabet \{a, b, ..., z\} are assigned with \{1, 2, ..., 26\}, respectively, and 27 denotes empty space. Message is transformed into a sequence \( \mathbf{m} \) with composite length 35, expressed as follows:

\[ \mathbf{m} = (20, 5, 13, 16, 5, 18, 1, 20, 21, 18, 5, 27, 9, 19, 27, 20, 23, 5, 14, 20, 25, 27, 4, 5, 7, 18, 5, 5, 19, 27, 14, 15, 23, 0, 0). \]

(42)

A degree-5 PGIS \( \mathbf{w} \) with period 5 is distributed in advance to the IoT platform, which is

\[ \mathbf{w} = (1 + 2j, 6 + 2j, 1 - 3j, 1 + 7j, -4 + 2j). \]

Because message \( \mathbf{m} \) has 35 elements, the upsampling factor is chosen to be 7. This implies that the secret encryption PGIS \( \mathbf{w}' \) is given by

\[ \mathbf{w}' = (1 + 2j, 0, 0, 0, 0, 0, 0, 6 + 2j, 0, 0, 0, 0, 0, 0, 1 - 3j, 0, 0, 0, 0, 0, 0, 0, 1 + 7j, 0, 0, 0, 0, 0, -4 + 2j, 0, 0, 0, 0, 0, 0). \]

(43)

The ciphertext obtained from taking circular convolution between message \( \mathbf{m} \) and encryption key \( \mathbf{w}' \) is given by

\[ \mathbf{c} = \mathbf{w}' \otimes \mathbf{m} = (108 + 226j, 107 + 234j, 53 + 236j, 98 + 86j, 67 + 154j, 7 + 179j, -45 + 2j, 78 + 266j, 2 + 39j, 23 + 101j, 103 + 56j, 42 + 149j, 42 + 129j, -70 + 125j, 78 + 221j, 162 + 264j, 138 + 151j, 38 + 91j, 132 + 264j, 72 + 14j, 120 + 95j, 153 + 226j, 42 + 74j, 118 + 121j, -2 + 151j, 42 + 64j, 152 + 149j, 175 + 10j, 148 + 191j, 72 + 159j, 33 + 121j, 3 + 96j, 152 + 239j, -130 + 49j, 70 + 70j). \]

(44)

Let "temperature is twenty degrees today" be the second message, where "now" of the first message is replaced by "today" to form the second message. Let \( \mathbf{m}_1 \) denote the transformed second message, where differences between two messages are underlined.

\[ \mathbf{m}_1 = (20, 5, 13, 16, 5, 18, 1, 20, 21, 18, 5, 27, 9, 19, 27, 20, 23, 5, 14, 20, 25, 27, 4, 5, 7, 18, 5, 5, 19, 27, 20, 15, 4, 1, 25). \]

(45)
\( c_1 = w' \otimes m_1 = \\
(108 + 226j, 107 + 234j, 89 + 248j, 98 + 86j, -47 + 116j, 13 + 181j, 105 + 250j, 78 + 266j, 2 + 39j, 29 + 83j, 103 + 56j, 23 + 206j, 43 + 126j, -45 + 50j, 78 + 221j, 162 + 264j, 144 + 193j, 38 + 91j, 113 + 131j, 73 + 21j, 145 + 270j, 153 + 226j, 42 + 74j, 94 + 133j, -2 + 151j, 118 + 26j, 148 + 151j, 75 + 60j, 148 + 191j, 72 + 159j, 39 + 133j, 3 + 96j, 133 + 201j, -12 + 51j, 95 + 120j). \) \( (46) \)

In (46), the number of Gaussian integers that are underlined is 15. These Gaussian integers are the same as those appeared in (44). The number of differences between \( m \) and \( m_1 \) is 5, while there are four times differences between \( c \) and \( c_1 \), which is 20. Even though the encryption key \( w' \) is with small period and has only five nonzero coefficients, it still achieves the goal of expanding differences between \( c \) and \( c_1 \) two ciphertexts. However, if PGIS \( s_{35} \), appeared in (18), is applied to encrypt these two messages, the entire contents of two ciphertexts \( c_2 \) and \( c_3 \), are extremely different.

\( c_2 = s_{35} \otimes m = \\
(-318 - 46j, -127 + 231j, -223 + 1719j, -828 + 2784j, 3 - 209j, -1102 + 2306j, -365 + 945j, 92 + 774j, -597 + 2091j, -6480 + 1744j, -703 + 1109j, -757 + 2121j, -377 + 2181j, -905 + 3015j, -403 + 1009j, -822 + 1466j, -813 + 2289j, -293 + 1929j, -212 + 936j, -1012 + 2836j, -1375 + 3125j, -393 + 1029j, 148 + 606j, -93 + 579j, -613 + 1639j, -612 + 836j, -477 + 1281j, -265 + 1845j, -23 + 369j, -907 + 2521j, -668 + 1004j, -883 + 2499j, -377 + 2181j, -212 + 936j, -340 + 820j). \) \( (47) \)

\( c_3 = s_{35} \otimes m_1 = \\
(-378 - 36j, -127 + 361j, 51 + 1977j, -838 + 2894j, -513 + 219j, -1148 + 2274j, -15 + 25j, 282 + 1284j, -607 + 2201j, -814 + 1122j, -763 + 1119j, -1023 + 3049j, -173 + 2649j, -565 + 2075j, -653 + 639j, -882 + 1476j, -729 + 2167j, -103 + 2439j, -488 + 1844j, -1248 + 2424j, -1085 + 2085j, -393 + 1159j, 338 + 1116j, -19 + 437j, -863 + 1269j, -938 + 1644j, -463 + 1369j, 275 + 1305j, -33 + 479j, -1157 + 2151j, -854 + 1392j, -883 + 2629j, 212 + 1494j, -243 + 1109j, -1115 + 2025j). \) \( (48) \)

The following example demonstrates that the same sparse PGIS \( w' \) does achieve the capacity of expanding differences to the resultant ciphertexts when two messages are similar. Let "the temperature is six degrees now" be the third message, and the first message is still "temperature is twenty degrees now".

\( m_3 = (20, 8, 5, 20, 5, 13, 16, 5, 18, 1, 20, 21, 18, 5, 27, 9, 19, 24, 7, 24, 5, 7, 18, 5, 19, 27, 14, 15, 23, 0, 0). \) \( (49) \)

\( c_4 = w' \otimes m_3 = \\
(168 + 196j, 111 + 157j, 109 + 158j, 64 + 278j, 96 + 177j, -45 + 110j, 25 + 195j, 63 + 236j, 61 + 117j, -26 + 43j, 54 + 138j, 16 + 147j, 65 + 115j, 10 + 125j, -12 + 191j, 136 + 227j, 24 + 133j, 154 + 153j, 101 + 262j, 110 + 25j, 50 + 20j, 138 + 271j, -24 + 82j, 69 + 108j, 149 + 178j, 66 + 92j, 90 + 65j, 170 + 155j, 133 + 86j, 46 + 177j, 44 - 2j, 24 + 143j, 151 + 182j, 5 + 135j, -5 + 5j). \) \( (50) \)

Though there exists no much difference between \( m \) and \( m_3 \), the contents of \( c_4 \) and \( c_3 \), from (44) and (50), which are encrypted by the same PGIS with 30 zero coefficients, are extremely different. We may consider the third message \( m_3 \) is similar to message permutation, which the permutation of message can achieve data protection to avoid attack. The final example demonstrates the actual result of message permutation. When the first three letters "twe" of "twenty" are moved to first three entries, the resultant message \( m_4 \) and cyphertext \( c_5 \) are given, respectively, as follows:

\( m_4 = (20, 23, 5, 20, 5, 13, 16, 5, 18, 1, 20, 21, 18, 5, 27, 9, 19, 27, 14, 20, 25, 27, 4, 5, 7, 18, 5, 19, 27, 14, 15, 23, 0, 0). \) \( (51) \)

\( c_5 = w' \otimes m_4 = \\
(168 + 196j, 126 + 187j, 109 + 158j, 64 + 278j, 91 + 142j, -34 + 187j, 26 + 202j, 63 + 236j, 151 + 47j, -26 + 43j, 54 + 138j, 36 + 137j, 21 + 137j, 6 + 127j, -12 + 191j, 151 + 182j, 24 + 133j, 154 + 153j, 96 + 252j, 121 + 47j, 51 + 22j, 138 + 271j, -9 + 187j, 69 + 108j, 149 + 178j, 36 + 82j, 156 + 87j, 176 + 157j, 133 + 86j, -14 + 207j, 44 - 2j, 24 + 143j, 146 + 197j, 16 + 102j, -4 + 2j). \) \( (52) \)

There are no common elements between \( c \) and \( c_5 \).

**IX. CONCLUSION**

This study proposes a novel hybrid public/private key cryptography based on circular convolution over a set of PGISs of period \( N = pq \). We show that circular convolution over PGISs is a trapdoor one-way permutation function involving the simultaneous performance of encryption and digital signatures. The abundant PGISs contribute to the high capacity of the associated cryptosystem; however, this system has the drawbacks of greater memory and bandwidth consumption. Data encryption using circular convolution is considered a vector-wise operation, thus it has more potential to achieve higher level of confidentiality than those private-key cryptography based on element-wise operation. In addition, circular convolution is equivalent to linear combination of message and its circular shifts, which is characterized by low computing load. These two properties make the proposed hybrid public/private key cryptography a candidate scheme for future lightweight cryptosystem.
REFERENCES

[1] M.S. Sharbaf, “Quantum cryptography: An emerging technology in network security,” 2011 IEEE International Conference on Technologies for Homeland Security (HST): pp. 13–19, 2011.

[2] R. L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” Communications of the ACM, 21 (2): pp. 120–126, 1978.

[3] W. Diffie and M. E. Hellman, “New directions in cryptography,” IEEE Trans. Inform. Theory, vol. 22, pp. 644–654, Nov. 1976.

[4] National Institute for Standards and Technology, “Digital signature standard (DSS),” Fed. Reg., vol. 56, p. 169, Aug. 1991.

[5] N. Koblitz, “Elliptic curve cryptosystems,” Math. Comput., vol. 48, no. 177, pp. 203–209, Jan. 1987.

[6] A. J. Menezes, Elliptic Curve Public Key Cryptosystems. Norwell, MA: Kluwer, 1993.

[7] W.-W. Hu, S.-H. Wang, and C.-P. Li, “Gaussian integer sequences with ideal periodic autocorrelation functions,” IEEE Trans. Signal Process., vol. 60, no. 11, pp. 6074–6079, Nov. 2012.

[8] Y. Yang, X. Tang, and Z. Zhou, “Perfect Gaussian integer sequences of odd prime length,” IEEE Signal Process. Letters., vol. 19, no. 10, pp. 615–618, Oct. 2012.

[9] X. Ma, Q. Wen, J. Zhang, and H. Zuo, “New perfect Gaussian integer sequences of period \( pq \), IEICE Trans. Fundam., vol. E96-A, no. 11, pp.2290–2293, Nov. 2013.

[10] H.-H. Chang, C.-P. Li, C.-D. Lee, S.-H. Wang, and T.-C. Wu, “Perfect Gaussian integer sequences of arbitrary composite length,” IEEE Trans. Inf. Theory, vol. 61, no. 7, pp. 4107–4115, Jul. 2015.

[11] C.-D. Lee, Y.-P. Huang, Y. Chang, and H.-H. Chang, “Perfect Gaussian integer sequences of odd period 2\(^k\) − 1,” IEEE Signal Process. Letters, vol.12, no.7, pp. 881–885, Jul. 2015.

[12] C.-D. Lee, C.-P. Li, H.-H. Chang, and S.-H. Wang, “Further results on degree-2 Perfect Gaussian integer sequences,” IET Commun., Vol. 10, no.12, pp. 1542–1552, Mar. 2016.

[13] S.-C. Pei and K.-W. Chang, “Perfect Gaussian Integer Sequences of Arbitrary Length,” IEEE Signal Process. Letters, vol.22, no.8, pp. 1040–1044, Jul. 2015.

[14] S.-H. Wang, C.-P. Li, H.-H. Chang, and C.-D. Lee, “A systematic method for constructing sparse Gaussian integer sequences with ideal periodic autocorrelation functions,” IEEE Trans. Communications, vol. 64, no. 1, pp. 365–376, Jan. 2016.

[15] C.-P. Li, S.-H. Wang, and C.-L. Wang, “Novel low-complexity SLM schemes for PAPR reduction in OFDM systems,” IEEE Trans. Signal Process., vol. 58, no. 5, pp. 2916–2921, May 2010.

[16] S.-H. Wang, C.-P. Li, K.-C. Lee, and H.-J Su, “A novel low-complexity precoded OFDM system with reduced PAPR,” IEEE Trans. Signal Process., vol. 63, no. 6, pp. 1368–1376, Mar., 2015.

[17] S.-H. Wang and C.-P. Li, “Novel comb spectrum CDMA system using perfect Gaussian integer sequences,” in Proc. IEEE Global Communications Conference (IEEE Globecom 2015), Dec. 2015.

[18] H.-H. Chang, S.-C. Lin, and C.-D. Lee, “A CDMA scheme based on perfect Gaussian integer sequences,” AEU International Journal of Electronics and Communications, vol. 75, pp. 70–81, May 2017.

[19] C.D. Lee and S. H. Hong, “Generation of long perfect Gaussian integer sequences,” IEEE Signal Processing Letters, vol. 24, no. 4, pp. 515–519, Apr. 2017.

[20] C.-D. Lee and Y.-H. Chen, “Families of Gaussian integer sequences with high energy efficiency,” IET Communications, vol. 10, no. 17, pp. 2416–2421, Nov. 2016.

[21] K.-J. Chang and H.-H. Chang, “Perfect Gaussian integer sequences of period \( p^k \) with degrees equal to or less than \( k + 1 \),” IEEE Trans. Communications, vol. 65, no.9, pp. 3723–3733, Sep. 2017.

[22] H.-H. Chang, K.-J. Chang, and C.-P. Li, “Construction of Period \( qp \) PGISs With Degrees Equal to or Larger Than Four,” IEEE Access, vol. 6, no. 1, pp. 64790-64800, Dec. 2018.

[23] P. Lancaster, Theory of Matrices, NY: Academic Press, 1969.

[24] P. J. Davis, Circulant Matrices. NY: Wiley-Interscience, 1979.

[25] B. Nobel and J. W. Daniel, Applied linear algebra. New Jersey: Prentice-Hall, Inc. 1988.

[26] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. CRC Press, Inc. 1996.