2019

The Chirp Function Revisited: A Uniqueness Conjecture for Chirplet Modulation

Jonathan Blackledge
Technological University Dublin, jonathan.blackledge@tudublin.ie

Paul Tobin
Technological University Dublin, paul.tobin@tudublin.ie

The Chirp Function Revisited: A Uniqueness Conjecture for Chirplet Modulation

J. M. Blackledge
Honorary Professor, Technological University Dublin
Professor Extraordinaire, University of Western Cape
Visiting Professor, University of Wales, Wrexham
jonathan.blackledge@dit.ie

P. Tobin
School of Electrical and Electronic Engineering
College of Engineering and Built Environment
Technological University Dublin, Ireland
paul.tobin@dit.ie

***Abstract*—The chirp function (a unit amplitude quadratic phase-only function with linear frequency modulation) is well known and is used in a wide range of applications including radar, digital communications, information coding and hiding and many other forms of signal and image processing. This is because the chirp provides an optimal solution to the problem of retrieving information from low energy signals with a low Signal-to-Noise Ratio (SNR). The chirp function also occurs in the solution to many mathematical models used to describe the propagation and scattering of waves (in the Fresnel zone), in quantum mechanics (the quantum shutter problem) and optical fiber communications to name but a few. In a 'systems and signals' context, the chirp function is accepted to be unique in that no other function has properties which yield such an optimal solution to the problem of extracting information from noise. In this context, we revisit the chirp function, consider a theorem and conjecture that attempt to quantify its unique properties through an analysis of its Fourier transform and re-establish the principles associated with the chirplet transform for functions of compact support. We then consider the principles of chirplet modulation for the transmission and reconstruction of bit-streams from signals with a low SNRs and show how this approach can be used to secure chirplet modulated signals using the prime number factorisation of a semi-prime derived from the value of the bandwidth of a communications channel.**

***Index Terms*—Chirp functions, chirplet transformation, uniqueness conjecture, deconvolution, chirplet modulation, prime number factorisation.**

I. Introduction

The unit amplitude linear frequency modulated chirp is defined by the function $\exp(i\alpha t^2)$ where $\alpha > 0$ is the 'chirp rate' which has units of time^{-2}). The chirp function is characterised by a quadratic phase function $\theta(t) = \alpha t^2$ and a linear frequency modulation of $2\alpha t$ (given by the derivative of the phase).

Chirp functions, chirplets (i.e. a windowed chirp function) and the chirplet transform [1] are re-occurring themes in the physical sciences. In signals and systems engineering, they have a range of applications including chirp spread spectrum methods which form part of the wireless telecommunications IEEE standards [2]. Other well-known applications include pulse compression designed to maximise the sensitivity and resolution of radar systems by modifying transmitted pulses to improve their auto-correlation properties using a chirp radar [3]. In the propagation of light pulses through optical fibers, spectral broadening and pulse compression can be extended to significantly higher pulse energies by using large-mode-area photonic crystal fibers in combination with chirping the input pulses [4]. In quantum mechanics, fundamental transient phenomena such as the the 'quantum shutter problem' [5] are characterised by a Fresnel integral, i.e. an integral whose kernel is characterised by a quadratic phase function. Chirped mirrors incorporate 'chirped spaces' in a dielectric designed to reflect wavelengths of light and compensate for dispersion effects that can be created by some optical elements [6]. More recently, in the field of cryptology, the chirp function has been used for key exchange [7], for the self-authentication of digital signals [8] and high resilience watermarking [9]. The chirp function even plays a role in cosmology given that gravity wave chirps are a principal signature for the detection of gravity waves generated by binary systems [10].

The examples given above are just a few of the many that can be considered to illustrate the importance of the chirp function, from its occurrence in characterising fundamental properties of the physical world to its applications in communications engineering (e.g. [11] and [12]). In this context, we re-consider the characteristics of the chirp showing that it has a conjugate Fourier eigenfunction, leading to the conjecture that this property is unique, i.e. no phase-only function other than the chirp has a conjugate eigenfunction. Coupled with the autocorrelation characteristics of a chirp function (which is also revised in this paper) this property underlies the uniqueness of the chirp function, and, in this context, we revisit the principles of transmitting information in the form of a bit-stream through a channel characterised by additive noise with a low SNR using a two-sided chirplet modulation algorithm. The accuracy of the demodulation scheme considered is quantified by examining the Bit-Error-Rate (BER). Finally, we explore a new communications protocol where, provided the sender and recipient of a chirplet modulated signal have accurate prior knowledge of the operational bandwidth, modulation and demodulation can be undertaken by factorising the value of a semi-prime (derived from the bandwidth) into two prime numbers. Providing the semi-prime is large enough, we briefly explore how this protocol yields the potential to exercise a

978-1-5386-6046-/18/$31.00

uniquely robust form of communications security, particularly in regard to the future development of quantum computing.

II. Uniqueness Conjecture

Theorem 2.1: Given the Fourier transform pair $F(\omega) \leftrightarrow f(t)$ where

$$F(\omega) = \int_{-\infty}^{\infty} f(t)\exp(-i\omega t)dt,$$

$$f(t) = \frac{1}{2\pi}\int_{-\infty}^{\infty} F(\omega)\exp(i\omega t)d\omega$$

and $F(\omega)$ exists if $f(t)$ is square integrable (i.e. $\|f(t)\|_2^2 < \infty$), then the phase-only function $f(t) = \exp(\pm it^2/2)$ has a conjugate phase-only eigenfunction that is unique.

Proof 2.1: It is well known that for a real constant α,

$$\exp(-\alpha t^2) \leftrightarrow \sqrt{\frac{\pi}{\alpha}}\exp[-\omega^2/(4\alpha)]$$

Hence, for $\alpha := \pm i\alpha$,

$$\exp(\pm i\alpha t^2) \leftrightarrow (1 \pm i)\sqrt{\pi}\exp[\mp i\omega/(4\alpha)]$$

and for the specific case when $\alpha = 2$, we obtain the conjugate eigenfunction relationship

$$\exp(\pm it^2/2) \leftrightarrow (1 \pm i)\sqrt{\pi}\exp(\mp i\omega/2) \tag{1}$$

where $(1 \pm i)\sqrt{\pi}$ is the (complex) eigenvalue. However, this approach does not express the uniqueness of the result. In order to do this we note that

$$\omega t = -\frac{1}{2}(\omega - t)^2 + \frac{\omega^2}{2} + \frac{t^2}{2}$$

so that we can write the Fourier transform in terms of the Bluestein decomposition [13]

$$\exp(i\omega^2/2)F(\omega) = \int_{-\infty}^{\infty} f(t)\exp[i(\omega - t)^2/2]\exp(-it^2/2)dt \tag{2}$$

Equation (2) is a fundamental result as it expresses the Fourier transform in terms of a convolution integral using chirp functions without loss of generality.

Consider the case where $f(t) = \exp(it^2/2)$ so that $f(t)\exp(-it^2/2) = 1$ and Equation (2) reduces to

$$\exp(i\omega^2/2)F(\omega) = \int_{-\infty}^{\infty} \exp[i(\omega - t)^2/2]dt$$

Since [14]

$$\int_{-\infty}^{\infty} \exp([i(\omega - t)^2/2)dt = (1 + i)\sqrt{\pi}$$

it is clear that

$$F(\omega) = (1 + i)\sqrt{\pi}\exp(-i\omega^2/2)$$

and hence we can write

$$\exp(it^2/2) \leftrightarrow (1 + i)\sqrt{\pi}\exp(-i\omega^2/2)$$

which generalises to

$$\exp(\pm it^2/2) \leftrightarrow (1 \pm i)\sqrt{\pi}\exp(\mp i\omega^2/2)$$

recovering the result given in Equation (1)

Remark 2.1: There are many examples of amplitude-only functions that are eigenfunctions of the Fourier transform, both periodic (such as the Dirac comb functions) and non-periodic (the most commonly quoted example being the Gaussian function). However, there appears to be no other phase-only function that has the same property (albeit of a conjugate type). This leads to the following conjecture.

Conjecture 2.1: The phase-only function $\exp[i\theta(t)]$ has a conjugate eigenfunction of its Fourier transform if $\theta(t) = \pm t^2/2$, and, more generally, if $\theta(t) = \pm(c + t^2/2)$ for constant c.

Remark 2.2: This conjecture is representative of at least one, but nevertheless, a fundamental property associated with the chirp function which is unique. However, the proof given above only applies to the case when $\theta(t) = \pm(c + t^2/2)$ and it has not been proven that there can be no other phase function except for $\pm(c + t^2/2)$ which has this property. In order to convert this uniqueness conjecture into a uniqueness theorem it must be proved that $\exp[i\theta(t)]$ has a conjugate eigenfunction of its Fourier transform if and only if $\theta(t) = \pm(c + t^2/2)$.

Remark 2.3: Introducing the chirp parameter α, it is noted that we obtained the self-characteristic relationship

$$\exp(\pm i\alpha t^2) \leftrightarrow (1 \pm i)\left(\frac{\pi}{2\alpha}\right)^{\frac{1}{2}}\exp(\mp i\omega^2/4\alpha) \tag{3}$$

III. The Chirplet Transform for Functions of Compact Support

Consider the chirplet transform of a function $f(t)$ of compact support, i.e. $f(t)\ \exists\ \forall t \in [-T/2, T/2]$, defined as

$$\exp(i\alpha t^2) \otimes f(t) = \int_{-T/2}^{T/2} \exp[i\alpha(t - \tau)^2]f(\tau)d\tau$$

where $\otimes$ denotes the (finite) convolution integral.

Theorem 3.1: The autocorrelation function $c(t)$ of the function $p(t) = \exp(i\alpha t^2),\ t \in [-T/2, T/2]$ is given by

$$c(t) = \exp(-i\alpha t^2) \odot \exp(i\alpha t^2) = \exp(-i\alpha t^2)T\mathrm{sinc}(\alpha Tt)$$

where $\mathrm{sinc}(x) \equiv \sin(x)/x$ and $\odot$ denotes the correlation integral.

Proof 3.1: The correlation function is given by

$$c(t) = \int_{-T/2}^{T/2} \exp[-i\alpha(t + \tau)^2]\exp(i\alpha\tau^2)d\tau = \exp(-i\alpha t^2)$$
$$\times \int_{-T/2}^{T/2} \exp(-2i\alpha t\tau)d\tau = \exp(-i\alpha t^2)T\mathrm{sinc}(\alpha Tt)$$

Corollary 3.1: Noting that

$$T\text{sinc}(\alpha T t) \leftrightarrow \frac{\pi}{\alpha}H(\omega),\ H(\omega) = \begin{cases} 1, & \mid \omega \mid \leq \alpha T; \\ 0, & \mid \omega \mid > \alpha T. \end{cases}$$

and from Equation (3), that

$$\exp(i\alpha t^2) \leftrightarrow (1+i)\left(\frac{\pi}{2\alpha}\right)^{\frac{1}{2}} \exp(-i\omega^2/4\alpha)$$

then, from the product theorem,

$$c(t) \leftrightarrow \frac{1}{2\pi}(1+i)\left(\frac{\pi}{2\alpha}\right)^{\frac{1}{2}} \exp(-i\omega^2/4\alpha) \otimes \frac{\pi}{\alpha}H(\omega)$$

Corollary 3.2: Noting that $c(t) \simeq T\text{sinc}(\alpha T t),\ \alpha T >> 1$, the spectrum of $c(t)$ is given by

$$C(\omega) \simeq \frac{\pi}{\alpha}H(\omega),\ \alpha T >> 1$$

Thus, when $\alpha T >> 1$, the bandwidth of the autocorrelation function is determined by αT alone and hence, for a chirp function of a finite extent (i.e. a chirplet), increasing the value of the chirp parameter α linearly increases the bandwidth of the auto-correlation function.

Remark 3.1: Theorem 3.1 and Corollaries 3.1 and 3.2 lead to the following result: If we chirplet transform an information function $f(t)$ and transmit the result in an environment characterised by an (additive) noise function denoted by random variable of time $r(t)$, say, such that the measured signal is given by

$$s(t) = p(t) \otimes f(t) + r(t)$$

then by correlating $s(t)$ with $p^*(t)$, we obtain an estimate $\hat{f}(t)$ for $f(t)$ given by

$$\hat{f}(t) = T\text{sinc}(\alpha T t) \otimes f(t) + p^*(t) \odot r(t),\ \alpha T >> 1$$

Since

$$T\text{sinc}(\alpha T t) \otimes f(t) \leftrightarrow \frac{\pi}{\alpha}H(\omega)F(\omega)$$

the information function is recovered with a bandwidth of αT subject to an additive perturbation compounded in the correlation function $p^*(t) \odot r(t)$. In other words $\hat{f}(t)$ is a band- and noise-limited version of $f(t)$ whose band-width is determined by αT subject to 'stochastic distortion' by $p^*(t) \odot r(t)$. Given that $p^*(t)$ and $r(t)$ are uncorrelated, then as $T \to \infty$, $p^*(t) \odot r(t) \to 0$ and hence

$$f(t) = p^*(t) \otimes s(t),\ T \to \infty$$

This result is the key to using chirplets in a range of applications including the one that is considered in the following section, and, coupled with Conjecture 2.1 identifies the chirp function as being unique in this respect.

IV. Discrete Chirplet Modulation

Let $f_n \equiv \{0,1\}^N$ denote a bit-stream composed of N bits. The function $f_n,\ n = 1, 2, ..., N$ is taken to be a binary representation of information where each 1 in the stream is a Kronecker delta function

$$\delta_{n-m} = \begin{cases} 1, & m = n; \\ 0, & m \neq n. \end{cases}$$

Two-sided chirplet modulating, we replace the bit-stream with a chirplet stream consisting of a concatenation of the functions $p_n^{\pm} = \pm\exp[i\alpha(n - T/2)^2],\ n \in [0, T]$ where p_n^+ 'encodes' '1' and p_n^- encodes '0'. Thus we consider a bit-to-chirplet stream transformation denoted by $\rightarrow$ which can be written in the form

$$\{0,1\}^N \rightarrow \{\text{cat}(p_n^{\pm})\}^{N \times T}$$

where

$$\text{cat}(p_n^{\pm}) = \begin{cases} p_n^{\pm}, & n \in [0, T]; \\ p_n^{\pm}, & n \in [T, 2T]; \\ p_n^{\pm}, & n \in [2T, 3T]; \\ \vdots & \\ p_n^{\pm}, & n \in [(N-1)T, NT]. \end{cases}$$

and cat denotes the concatenation of $p_n^{\pm}$. The j^{th} bit, $f_n,\ n = 1, 2, ..., N$, in the bit-stream $\{0,1\}^N$ therefore transforms to the j^{th} chirplet in the chirplet stream, the output being taken to be the real component of $\text{cat}(p_n^{\pm})$.

'Chirp modulating' a bit-stream in this way allows each bit to be recovered by correlating the stream with the complex conjugate of, and critically, an identical chirp function p_n^+. Thus we can write the output of this correlation as

$$s_n = (p_n^+)^* \odot \text{Re}[\text{cat}(p_n^{\pm})] \sim \text{cat}(\delta_{n-m}^{\pm})$$

where

$$\delta_{n-m}^{\pm} = \begin{cases} \pm 1, & m = n; \\ 0, & m \neq n. \end{cases}$$

A further process is then required to convert the Kronecker δ-stream back to the original bit-stream, i.e.

$$\{\text{cat}(\delta_{n-m}^{\pm})\}^{N \times T} \rightarrow \{0,1\}^N$$

Since each reconstructed Kronecker delta will be positive or negative at positions $(mT/2) - 1,\ m = 1, 3, 5, ...$ where T is an even integer, this can be accomplished through application of the following process:

$$\forall j \in [1, N]: \begin{cases} \text{if } \text{Re}[s_{n=[(2j-1)T/2]-1}] \geq 0, & f_j = 1; \\ \text{if } \text{Re}[s_{n=[(2j-1)T/2]-1}] < 0, & f_j = 0. \end{cases}$$

from which the original bit-stream $\{0,1\}^N$ is recovered.

In practice, the value of T determines the array length used to compute the discrete chirplet. Given T, a value of α must be chosen that avoids aliasing. To obtain a non-aliasing criterion for the value of α given T, we note that from Corollary 3.2, the

autocorrelation of $\exp(i\alpha t),\ t \in [-T/2, T/2]$ has a bandwidth $\sim \alpha T,\ \alpha T >> 1$. Hence, under the same condition, the bandwidth of $\exp(i\alpha t^2)$ is also of the order of αT. From the sampling theorem, it is then clear that if Δ denotes the sampling interval, then $\Delta \leq 1/2\alpha T$ and thus, for $\Delta = 1$, $\alpha \leq 1/2T$ where $\alpha = 1/2T$ provides a Nyquist sampled chirplet.

Chirplet modulation of each bit, as opposed to chirplet transforming the bit-stream in its entirety, provides the potential for generating greater 're-constructive power' of each bit in the stream. This approach comes at the computational 'cost' of expanding the length N of the bit-stream to a chirp-stream of length $N \times T$. If we consider the transmission of a chirp-stream in an additive noisy environment when we record a (real) digital signal of the form (for $n = 1, 2, ..., NT$)

$$s_n = \mathbf{SNR} \times \mathrm{Re}[\mathrm{cat}(p_n^{\pm})] + r_n,\ \|r_n\|_\infty = 1 \qquad (4)$$

then, in the context of Conjecture 2.1 and the results discussed in Remark 3.1, we can consider the reconstruction of any element of f_n (with bandwidth of αT) from s_n to be uniquely optimal.

In a communications system, the two-sided base-band function $\mathrm{cat}(p_n^{\pm})$ is assumed to be frequency modulated (after D-to-A conversion) for the purpose of transmission and that the (digital) signal s_n given in Equation (4) is therefore assumed to be the result of frequency demodulation back to baseband followed by A-to-D conversion. The noise function r_n therefore depends on the noise that is characteristic of the sideband with frequency range $\omega_0 - \alpha T/2$ to $\omega_0 + \alpha T/2$ for carrier frequency ω_0 in which the (frequency modulated) transmission takes place. It is this bandwidth that determines the noise type and SNR of the base-band signal, i.e. the statistical distribution of r_n and the value of SNR in Equation (4). The algorithms considered in the following section are designed to test this approach and thereby investigate the BER associated with the reconstruction of f_n from s_n for decreasing values of the SNR.

V. Numerical Implementation based on Prototype MATLAB functions

The modulation and demodulation processes discussed in Section IV are implemented in MATLAB functions CM (Chirplet Modulation) and CD (Chirp Demodulation) given in Appendix A for zero-mean, normally distributed noise. The functions have been commented to provide a narrative on their composition which reflects the processes (and notation) presented in Section IV using a Nyquist sampled chirplet. By way of an example, consider Figure 1 which shows plots of the real component of the two-sided chirp function $\mathrm{Re}[p_n^{+}]$, the functions $\mathrm{Re}[\mathrm{cat}(p_n^{\pm})]$ and s_n given in Equation (4) and the demodulated signal for the input bit-stream $\{0, 1, 0\}$. These results are based on running the MATLAB functions given in Appendix A for $T = 400$ and $\mathrm{SNR} = 0.1$, i.e. CM(400,0.1) and CD(400). The BER defined by

$$\mathrm{BER} = \frac{1}{N} \sum_{j=1}^{N} |\ f_j - \hat{f}_j\ |$$

where f_j and $\hat{f}_j$ denote the input bit-stream to function CM and the output bit-stream obtained from function CD after demodulation, receptively, is zero.

Figure 2 shows the BER for a range of values of $\mathrm{SNR_{dB}} = 10 \log_{10} \mathrm{SNR}$ (Decibel scale - dB) for $T = 400$. The input used to generate this plot is the (ASCII) binary string for the sentence 'BER test for chirplet modulation method.' and illustrates that, in this case, as $\mathrm{SNR_{dB}}$ decreases (from -15 dB to -30 dB), the BER becomes increasingly high. From $\sim$ -15 dB to 0 dB, the BER is zero.

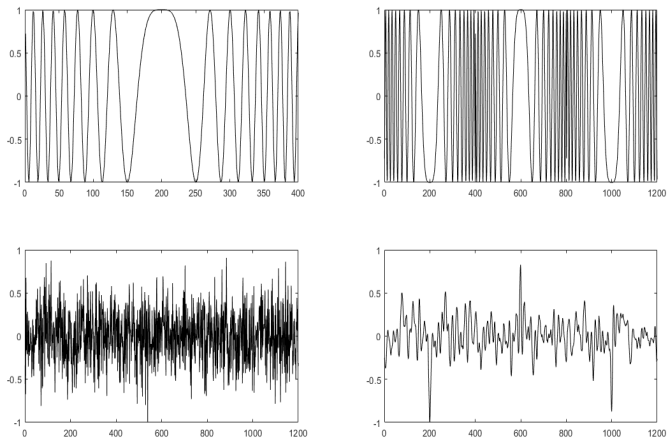

Fig. 1. Plots of the two-sided chirp function (top-left), chip modulated signal - the 'chirp stream' (top-right), chirp modulated signal with normally distributed additive noise (bottom-left) and the signal after demodulation (bottom-right) for CM(400,0.1) and CD(400).

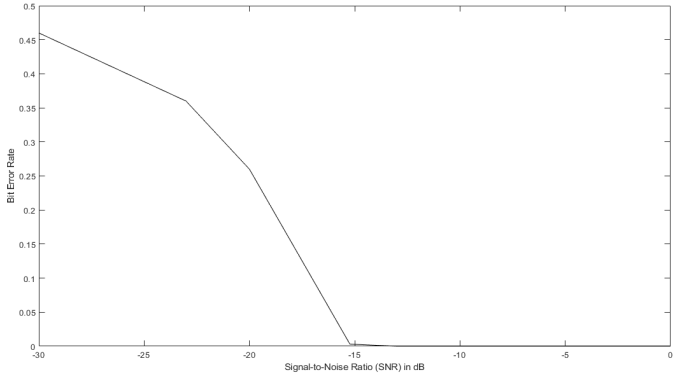

Fig. 2. Plot of the BER for different values of the $\mathrm{SNR_{dB}} = 10 \log_{10} \mathrm{SNR}$.

VI. Prime Number Factorisation of Angular Bandwidth

The 'key' to demodulating the signal s_n given by Equation (4) is the value of T. In this section, we consider a protocol in which sender (Alice) and receiver (Bob) can generate T without having to apply a separate key exchange algorithm and is based on knowledge of the bandwidth of the communications channel after frequency modulating s_n (upon D-to-A conversion). It is an approach that lends itself

to the application of a quantum computer for factorising large prime numbers using Shor's algorithm [16]. In this context, the protocol introduces a high level of security in association with chirplet modulation provided that both Alice and Bob have a quantum computer to factorise a large prime number derived from the bandwidth of the communication channel as shall now be discussed.

Let B be the bandwidth in Hz available for Alice to communicate to Bob and let us write this number in the form

$$B = b_1.b_2b_3...b_n = b_1b_2b_3...b_n \times 10^{-(n-1)}$$

where b_j denotes any one of the base 10 digits (0,1,2,...,9) and $b_1b_2b_3...b_n$ is the signifcand consisting of n digits, the value of n being taken to be determined by the decimal accuracy available to both Alice and Bob. We then find the largest pair, and only the pair, of prime numbers p and q such that the semi-prime pq is given by $pq = b_1b_2b_3...b_m,\ m \leq n$ where $n-m$ is a minimum. This is achieved by systematically reducing the number of digits $b_1b_2b_3...b_n$ (from right to left) one digit at time and decomposing the integer obtained into a product of prime numbers (given that any positive integer can be decomposed into a product of prime numbers) until the first two prime number factorisation is achieved. We then compute the decimal number

$$D = \frac{p}{q},\ p > q \text{ or } D = \frac{q}{p},\ q > p$$

so that $D = d_1.d_2d_3...,$ where $d_1 \geq 1$ Finally, applying an upper bound to the value of T given by $T \leq 10^L$, say, where L is a positive integer, we set $T = d_1d_2d_3...d_L$. The larger the value of L the greater the computational time required to modulate and demodulate. A bit-stream of size N yields a chirp-stream of size $NT \leq NL$. For demodulation, the direct correlation process used in function CD requires $\sim NL^2$ floating point multiplications (and additions). While this can be reduced to $\sim NL\log_2 L$ by using a Fast Fourier Transform, it is clear that the value of L needs to be kept to a minimum in order to reduce the computational overhead. This of course depends upon the computational power available to Alice and Bob.

A. Numerical Example

To illustrate the protocol, suppose Alice and Bob wish to communicate through a component of the electromagnetic spectrum in frequency range 1.42 - 1.67 GHz giving an available bandwidth of B=0.25 GHz. Assuming that Alice and Bob can process data with a maximum floating point precision of 16 digits, say, then $\alpha T = 2\pi \times B = 1.570796326794897$. In this case, prime number decomposition yields

$$1570796326794897 = 2 \times 3 \times 751 \times 348601049;$$
$$157079632679489 = 13 \times 12083048667653.$$
$$\Rightarrow 1.3 \times 1.2083048667653 = 1.570796326794890 \text{ and}$$
$$D = 12083048667653/13 = 9.294652821271538 \times 10^{11}.$$

With $L = 3$, $T = 929$ and $\alpha = 1/2T = 5.3821 \times 10^{-4}$.

In this case, subject to L having been set by both parties, Bob only needs to know the operational bandwidth B, say (which needs to be known by default) and the prime number factorisation rule that Alice applies. The principal point here, is that the angular bandwidth can be defined with high decimal point precision. This is because, provided B is taken to be a rational number, then the angular bandwidth $2\pi B$ is an irrational number because π is an irrational number. Thus, the bandwidth can be specified to any decimal accuracy, limited only by the floating point accuracy available to Alice and Bob, thereby increasing the size of the prime numbers required.

B. Discussion

The protocol provides the potential for using Shor's algorithm implemented on a quantum computer to generate prime numbers when the angular band-width is specified as a decimal number with enough digits to make the semi-prime representation unable to be factored using conventional digital computing. Prime number factorisation is of particular significance in regard to quantum computing and the application of Shor's algorithm and developments thereof [17]. It is therefore conceivable that, at some future date, Alice and Bob could use chirplet modulation using semi-prime representations of $2\pi B$ with 1000++ decimal digits, if they both have access to a quantum computer to implement Shor's algorithm. The security of such a communications protocol is self-evident especially when computational facilities are available to chirplet modulated and demodulate for large L.

VII. Conclusions

In revisiting the chirp function we have developed the conjecture that there is a unique phase-only function that has a conjugate eigenfunction upon Fourier transformation, namely, the function $\exp(\pm it^2/2)$. We have considered an algorithm to chirplet modulate a bit-stream (using a two-sided chirplet) and briefly demonstrated the numerical performance of the MATLAB functions provided in Appendix A designed to test the process, showing that a zero BER can be achieved subject to relatively low values of the SNR as illustrated in Figure 2. We have further considered a protocol based on the prime number factorisation of the bandwidth by treating its signifcand as a semi-prime, thereby securing the 'key' to generating the Nyquist sampled chirplet required to demodulate a chirplet modulated signal, i.e. a Nyquist sampled chirplet of length T. Finally, given that chirplet modulation provides a uniquely optimal solution for communicating information in a noisy environment with a low SNR, we note that in the example given in Section VI.A, the bandwidth considered has not been chosen arbitrarily; it is the bandwidth of the 'Waterhole' [18]. In this context, we imply that the analysis and interpretation of SETI signals might be well served using chirp demodulation for different values of T and the output binary strings processed using entropy-conscious machine learning algorithms designed to differentiate between random and non-random binary strings.

APPENDIX A
MATLAB FUNCTIONS FOR CHIRPLET MODULATION

The functions given in this Appendix have not been exhaustively tested and have no data error checks. They are provided to give the reader a guide to the basic programming required to implement the computational procedures discussed in Section IV. The code given has been condensed in order to comply with the prescribed page limit of this publication.

Function CM - Chirp Modulation

```
function []=CM(T,SNR)
%INPUTS: int T - chirplet array size.
%double SNR - Signal-to-Noise Ratio.
%Read bitstream from file 'bits.txt'.
fid=fopen('bits.txt','r'); f=fread(fid);
fclose(fid); N=size(f,1);%Compute size.
%Convert f (composed of values 48 & 49)
%into an array composed of values -1 & 1.
for n=1:N temp=f(n); if temp==48, K(n)=-1;
else K(n)=1; end
end %Compute Nyquist sampled chirplet of
%length T where if T is odd, T set to T+1.
if mod(T,2)==1 T=T+1; end
for n=1:T t(n)=n-(T/2); end
alpha=1/(2*T); p=complex(cos ...
(alpha*t.*t), sin(alpha*t.*t));
%Chirp modulate the bit array
for k=1:N for j=1:T
s(j,k)=K(k)*p(j); end
end %Concatenate, returning reals.
s=real(s(:)); s=s/max(s); %Normalise.
%Compute normally distributed random
%numbers and normalise.
NT=size(s,1); r=randn(1,NT)';
r=r/max(abs(r));
%Add noise using SNR and write s to file.
s=SNR*s+r; dlmwrite('cm.txt',s);
```

Function CD - Chirp Demodulation

```
function []=CD(T)
%INPUTS: int T - chirplet array size
%Read chirplet modulated data
s=dlmread('cm.txt');
%Compute chirplet checking to see
%if T is odd (when T is set to 1+T).
if mod(T,2)==1 T=T+1; end
for n=1:T t(n)=n-(T/2); end
alpha=1/(2*T); p=complex(cos ...
(alpha*t.*t), sin(alpha*t.*t));
%Demodulate using a flipped convolution
%with a conjugated chirplet, renormalise
%the result and output the reals.
d=conv(s,conj(fliplr(p)),'same');
d=d/max(abs(d)); d=real(d);
%Recover bit array by checking polarity
%of array d for elements at the centre
%of each chirplet at N/2-1, 3*N/2-1, ...
NT=size(d,1); %Compute size of d.
step=round(NT/T);%Compute step size.
j=1; %Start array processing.
for k=1:step K=2*k-1; temp=d(K*(T/2)-1);
if temp < 0 f(j)=0; j=j+1; end
if temp >= 0 f(j)=1; j=j+1; end
end %and write result to file 'cd'.
fid=fopen('cd.txt','w');
fprintf(fid,'%d',f); fclose(fid);
```


ACKNOWLEDGMENTS

The authors would like to acknowledge the support of the Technological University Dublin, the University of Western Cape and Wrexham Glyndrw University.

REFERENCES

[1] S. Mann and S. Haykin, *The Chirplet Transform: Physical Considerations*, IEEE Transactions on Signal Processing, vol. 43, no. 11, 27452761, 1995

[2] IEEE Computer Society, IEEE Standard 802.15.4a-2007, 2007.https://ieeexplore.ieee.org/document/4299496

[3] J. R. Klauder, A. C. Price, S. Darlington and W. J. Albersheim, *The Theory and Design of Chirp Radars*, Bell System Technical Journal, vol. 39, issue 4, 745808, 1960. https://ieeexplore.ieee.org/document/6773600

[4] P. Dombi, P. Racz, L. Veisz and P. Baum, *Conversion of Chirp in Fiber Compression*, Optics Letters, vol. 39, no. 8, 2014. http://real.mtak.hu/23578/1/Dombi_FiChirpConv_OL.pdf

[5] M. Moshinsky, *Diffraction in Time*, Physical Review, vol. 88, no. 625, 1952.

[6] C. Q. Cook and A. Ariel *Theory of Chirped Photonic Crystals in Biological Broadband Reflectors* Optica, vol. 3, issue 12, 1436-1439, 2016. *https://doi.org/10.1364/OPTICA.3.001436*.

[7] A. Al-Ismaili, *Dynamic Block Encryption with Self-Authenticating Key Exchange*, PhD Thesis, Loughborough University, 2006.

[8] J. M. Blackledge, *Cryptography and Steganography: New Algorithms and Applications*, Lecture Notes, Centre for Advanced Studies, Warsaw University of Technology, Warsaw, 2012, ISBN: 978-83-61993-05-6;https://arrow.dit.ie/engscheleart2/40/

[9] J. M. Blackledge and O. Iakovenko, *Resilient Digital Watermarking for Document Authentication*, IAENG International Journal of Computer Science, vol. 41, no. 1, 1-17, 2014.

[10] V. Tiwari, S. Klimenko, V. Necula and G. Mitselmakher*Reconstruction of Chirp Mass in the Search of Compact Binaries*, Classical and Quantum Gravity, vol. 33, no. 1, 2016. https://arxiv.org/abs/1510.02426

[11] S. Darlington, *Chirp Pulse Transmission*, US Patent 2678997, May 18, 1954

[12] S Darlington, *Chirp Pulse Equalisation*, US Patent 3618095, Nov. 11, 1969

[13] L. Bluestein, *A Linear Filtering Approach to the Computation of Discrete Fourier Transform*, IEEE Transactions on Audio and Electroacoustics, vol. 18, issue 4, 451455, 1970. https://ieeexplore.ieee.org/document/1162132

[14] Integral Caculator, *Calculate Integrals Online - with Steps and Graphing*, 2019. https://www.integral-calculator.com/

[15] R. Rivest, A. Shamir and L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems* (PDF). Communications of the ACM, vol. 21, no. 2, 120126, 1978. https://dl.acm.org/citation.cfm?doid=359340.359342

[16] P. W. Shor, P*Algorithms for Quantum Computation: dDiscrete Logarithms and fFactoring*, Proceedings 35th Annual Symposium on Foundations of Computer Science, 1994. https://ieeexplore.ieee.org/document/365700

[17] D. J. Bernstein, N. Heninger, P. Lou and L. Valenta, *Post-quantum RSA*, International Workshop on Post-Quantum Cryptography: 311329, 2017. https://cr.yp.to/papers/pqrsa-20170419.pdf

[18] The SETI League Inc, General Information *What Is the Water-Hole?*, 2019. http://www.setileague.org/general