TYLER BURGEE, Department of Computer Sciences, Mathematics, and Engineering, Shepherd University, Shepherdstown, WV, 25443. Superposition as a Means of Data Encryption in N-Dimensional Value Spaces.

The objective of this study was to provide a new method for creating quantum-proof encryption algorithms. I accomplished this by designing a symmetric 2-key cryptosystem that exploits the superposition principle to encrypt data in multi-dimensional value spaces.

The proposed cryptosystem substitutes characters for frequencies, as determined by two private keys: component wave order key (CWOK) and character transmission order key (CTOK). A CWOK defines the values and theoretical spatial arrangement of frequencies in a complex wave. A CTOK defines the unique arrangement of system characters (i.e., characters in an encoding scheme such as ASCII), determined by a hash function, to identify a user. Combining the CWOK and CTOK, we construct a character-lookup table (CLT), which defines the character-frequency relationships used to generate a substitution cipher. A cipher's frequency values must be superimposed in accordance with the CWOK. Fast Fourier Transforms are used during the decryption stage to perform complex wave analysis.

Complex waves can have $n!$ frequency configurations, where n = *the number of component frequencies*; each CTOK can have $a!$ character configurations, where a = *the number of characters defined in an encoding scheme*. Therefore, by requiring $n \geq 128$ and using the ASCII encoding scheme ($a = 128$), there are $n!+a!=128!+128!=2*128!$ possible key configurations for any given cipher. This is approximately $3.330284e+138$ times as many key configurations possible with AES 256.

Exploiting the multi-dimensional nature of complex waves, and combining these techniques with other powerful encryption algorithms used today, it appears likely that we can create a quantum-proof cryptosystem.