Backchannelling Quantum bit (qubit) 'shuffling'

Quantum bit (qubit) 'shuffling' as added security by slipstreaming Q–Morse

Dr John Ronczka
SCOTTYNCC Independent Research Scientists
Australia
ronczkaj@ozemail.com.au

***Abstract*—A fresh look at the way secure communications is currently being done has been undertaken as a consequence of the large hacking's that have taken place recently. A plausible option maybe a return to the future via Morse code using how a quantum bit (Qubit) reacts when entangled to suggest a cypher. This quantum cyphers uses multiple properties of unique entities that have many random radicals which makes hacking more difficult that traditional 'Rivest-Shamir-Adleman' (RSA), 'Digital Signature Algorithm' (DSA) or 'Elliptic Curve Digital Signature Algorithm' (ECDSA). Additional security is likely by Backchannelling (slipstreaming) Quantum Morse code (Q–Morse) keys composed of living and non-living entities. This means Blockchain ledger history (forwards—backwards) is audited during an active session. Verification keys are Backchannelling (slipstreaming) during the session (e.g. train driver must incrementally activate a switch otherwise the train stops) using predicted— expected sender—receiver properties as well as their past history of disconformities to random radicals encountered. In summary, Quantum Morse code (Q–Morse) plausibly is the enabler to additional security by Backchannelling (slipstreaming) during a communications session.**

Keywords—Cypher; Quantum bit (Qubit); entanglement;; shuffling; Morse; containment wave; Backchannelling.

I. INTRODUCTION

Obtaining increased security layers for a variety of sensors to devices in the 'Internet of Things' (IOT) to the 'Internet of Everything' (IOE) is a current issue. Let's take a journey into how quantum information in the context of qubit 'shuffling' might make communications more secure.

A. Nature of its technical/scientific contribution

The intent is to provide a 'Backchannelling' cypher that can be tailored to the unique properties of both the utilised devices to message sender and receiver. Increase security for autonomies robotic and systems is a requirement due to the open source ecosystem. Particular attention is likely to be given to 'Simultaneous Localization And Mapping' (SLAM) and 'Robot operating system' (ROS) to ensure intended entity use only [1] [2].

Another is the cascade of the numbers of sensors and devices integrating within the 'Internet of Things' (IOT) and with Precision Agriculture potentially the 'Internet of Everything' (IOE). A more secure robotic and systems ecosystem including the supporting C5I4 continuum ('Command—Control—Communications—Computers—Collaboration—Intelligence—Information—Integration—Interoperability') appears required. As such there are unmet 'needs' (must have) and 'wants' (nice to have) to ensure future robotic autonomies developments are orientated and adaptable for both earth and space operations.

B. Problems

Secure communications has become an important consideration with the multiple sensors and devices being used and being hacked recently. A cautionary note is that increased security layers have needs (must have) and wants (should—nice to have) to be met that slows the response times but attempts to negate third party hackings. A refreshing of the paradigms and algorithm's used for security have been prompted by recent extensive 'distributed denial-of-service' (DDoS) and calls for 'end-to-end' (E2E) encryption. Recent technology news report of DDoS events suggests that redundant devices were hacked with unintended consequences for the more up-to-date parts of the 'Internet of Things' (IOT). These older devices may be the biggest concern and threat that needs to be addressed [3] [4].

C. Domains or environments to which it is applicable

Within robotics autonomies engineering, there appears to be the used of various old and new technologies, sensor and devices. The issue relates to the vulnerabilities that the use of a mixed old—new ecosystem brings with the growth of the 'Internet of Things' (IOT) to the 'Internet of Everything' (IOE). By addressing the vulnerabilities associated with the open source nature of the operating environment a more secure and intuitive outcome might be achieved.

II. BACKGROUND

A. Backchannelling

Within the social interaction ecosystem a conversation maybe by a sender and then a receiver who tends to confirm the level of understanding (backchannel). Therefore, backchannelling may use semantic (linguistic), semiotic (symbol, action) or both and undertaken as a face–to–face or via a communications interface device simultaneously. This process might be translated into the 'Artificial Intelligence' (AI) and 'Artificial Wisdom Intelligence' (AWI) context in robotics autonomies systems and social devices [4].

978-1-5090-5753-5/16 $31.00 © 2016 IEEE
DOI 10.1109/APWC.on.CSE.2016.26

B. Cypher?

A cypher (also known as 'cipher') provides a means for a sender to hide the true message via a unique encrypting key (e.g. shift; substitution; polyalphabetic; transposition). The receiver to understand the encrypted message uses a unique decryption key but interdiction by a 'man–in–the–middle' (MITM) should be considered (break the key) by using methodical techniques such as patterning. As a countermeasure the sender might use complex algorithms with 'one–time–keys' (OTK) that have short expiry times [5] [6].

There appears to be a number of types of Keys algorithm's that are used to change the plain text via a cypher to get an encrypted message. Of note are the 'Rivest-Shamir-Adleman (RSA: signature; verification; encryption), Digital Signature Algorithm (DSA: signature; verification; decryption) and 'Elliptic Curve Digital Signature Algorithm' (ECDSA). A Master key might be used to further encrypt these keys (Public (e.g. host system; passphrase: password); Private (e.g. Logon - credit Card; passphrase: PIN)) for an additional security layer There is a balancing decision of the security level versus the system 'quality of service' (QOS) [7] [8] [9] [10] [11] [12].

C. Quantum Cypher?

There might be a disconformity in relation to Quantum computing benefits (speed; resolving complex problem) and dis-benefits (data security; breaking encrypted keys). The outcome desired is secure encrypted private and public keys known as a 'Quantum Key Distribution' (QKD) based. This focuses on use of entanglement properties and any relevant lessons learn ('quantum bit error rate (QBER)). A starting point was the initial protocols developments in 1984 by 'Bennett and Brassard' (BB84) that was based on photons (various polarization states) and then pushing backchannelling verification during an active session as added security.

Pushing backchannelling verification could move cryptographies from a step by approach to a combination of multiplexing Blockchains (Transaction data linked but decentralized and network shared) audit using bits, quantum qubits and other properties. In summary Quantum computing instils a paradigm shift in how cyphers have and will work into the future (rapid cycling of changes). The desired outcome is to gain secure and integral C5I4 ('Command—Control—Communications—Computers—Collaboration—Intelligence—Information—Integration—Interoperability'), with physical space and time before discovery [12] [13] [14] [15] [16]

D. Spintronics as an enabler

Spintronics also known as 'Spin electronic' relates to the transport of electrons by spinning based on dynamics in current—magnetic—electronic properties and different up—down states. In pushing backchannelling verification spintronics is the applications enabler together with new cyphers for 'Quantum Key Distribution' (QKD).

The associated processes and conceptualization (e.g. Zeeman effect; diffusion; Hall effect; Schottky barrier) may be an enabler to understanding quantum qubit shuffling. There are key security linkages that might relate to changes in negative and positive states and electric fields of the electrons and the nexus with information storage and transmission.

By understanding spintronics, electrical profile (voltage and current charges) and the associated magnetic flux relationships it is likely to move to a new paradigm for large secure data storage technologies. What is of particular interest in the use of Spinmechatronics structures based on transistors for magnetic–tunneling layer stacking. The second relates to spin waves (magnonic; polarized; cycloidal; frequencies than can be turned) develop a more secure, environmentally friendly and sustainable sensors and devices [17] [18] [20] [21].

E. Electromagnetism

Electromagnetism appears to be the key to 'shuffling', rotation of the quantum bit's (qubit's) and unique direction of the magnetic flux. One such hybrid approach is based on Lloyd's qubit conceptualization that contains magnetic field direction reversal as current reverses and current size proportional to magnetic field strength [22] [23] [24].

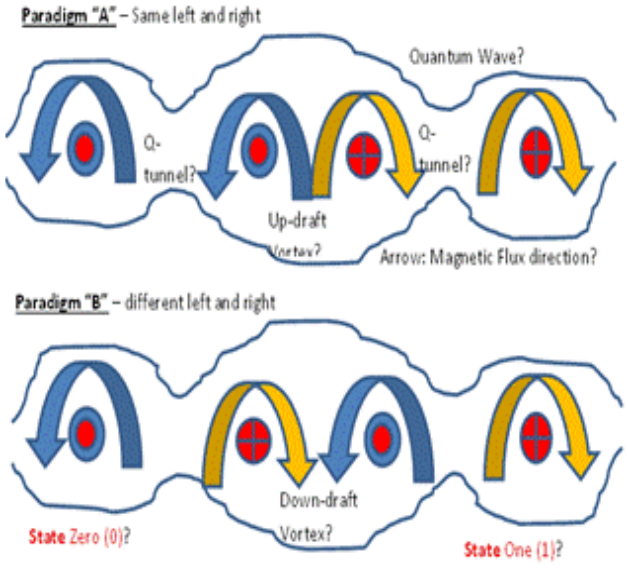
F. Information within a containment

Generally increased security tends unfortunately not be progressive incremental change but progressed by reactions to large data breaches to virus threats. Substandard architectural designs and level of capability to detect and then response in a timely way could contribute to the way the breaches cascade. One security approach is to use containment of sensitive information packets each with unique properties such as quantum qubit shuffling to entanglement as well a user—sender biometrics and bio profiles. Such an architecture design tends to have many logic gates that combine as 'causality logic gate delivery engines' that may be part of a systems control management system. The important drivers might be signal containment scaffolds with quantum bit properties and nexus with Blockchains. Likely tools link to using 'Quantum Key Distribution' (QKD) based 'Artificial Wisdom Intelligence' (AWI) (Attachment 'A').

Another relates to Infosphere (information within containment) waves of magnetic flux (Paradigm "A": Same left and right; Paradigm "B": different left and right) as seen in Figure 1. It might have a signaling scaffolding that is formed by spooling (like a sail sheet winding tightly) of signal packets to establishing a quantum wave to access a nexus entanglement. Foundation concepts are:

- **Paradox influences: '***de Montaigne': 'nothing is so firmly believed as that which we least know'*
- **C5I4:** C5I4 continuum ('Command—Control—Communications—Computers—Collaboration—Intelligence—Information—Integration—Interoperability')
- **CPPWSRVC:** algorithms that 'calibrates—push—pull—wait—swap—recalibrate—verification—cascades' (CPPWSRVC)
- **A6:** applicable as 'anywhere—anytime—anyplace—anydevice—anycomms—anyentity' (A6).
- **CSIANS:** ('calibration, synergy, integration, assimilation narrative and synchronization')

- **PARRIFA:** 'Debt to be paid': 'portability—agility—redundancies—responsiveness—insight—foresight—adaptability' (PARRIFA)



a.

Fig. 1. Quantum qubit shuffling (containment wave)

G. Cyphers for Quantum deception

Message interdiction by third parties would not be a surprising occurrence in today's communications environment. It is therefore a desirable deliverable to safeguard the 'point–to–point' (P2P) session (unique 'Media access control' (MAC) address established) and message in the most secure manner (encryption). To reduce the risk of inappropriate third party ('man–in–the–middle' (MITM)) decrypting via single event entanglements ('one time keys' or 'one time pads'). A required intervention—countermeasure might be nested with long strings with packet switching (breaking up; multiple path); multi frequency hopping transmission-reassembling to use of containment waves and pushing backchannelling verification. The enstate is to negate an inappropriate third party ('man–in–the–middle' (MITM)) interdiction by the collection of the typology of the message in order to gain time and space before decryption is made.

One may suggest that accepting the dilemma that the concept that a quantum computer provides speed and flexibility particularly when used with 'Artificial Intelligence' (AI) will plausibly be able to defeat an 'Quantum Key Distribution' (QKD) encrypted message. This inclines one to believe the deliverable appears to be achieving the required time and space before decryption is made. The other problem arises as both authorizes sender—receiver and the hackers are tending the use similar tools. A way forward is likely to push, pull and cascade a type of cloaking of the cypher and public keys being used with deliberate random radical frequency changes, illogical algorithms, and signaling noise ('Signal-to-Noise Ratio' (SNR)) errors [6]. [5] [25] [26].

H. Slipstreaming

Within a communication backbone together with blockchaining there might be residual breadcrumbs and handshakes (before during and after) as fractal evidence (forensics) that may be reconstructed—repurposed—reused? It could be simple process (e.g. detect, interdict by shaping entry vectors and data manifold's (Infiltration—Exfiltration Multiplexing)).

Entanglement slipstreaming (moving over-under-between (scaffolding)) is suggested to be both an intervention and countermeasure whilst a host P2P interdiction is occurring. As the forward signal is being enacted (whilst host is communicating P2P) a 'slipstreaming' event ('Backchannelling' the infiltration—exfiltration) is an audit check against the available Blockchain and signal linkage acceptable operating parameters. That is, simultaneously intervention—countermeasure (Attachment 'A': C5I4—A6—CSIANS—PARRIFA) via the established secure communications channel with a base primer (host P2P signal). The outcome is to backchannel (slipstreaming) without further effort but still be able to handed off (handshake) to another but still maintain a communication and decoded message access. The backchannel (slipstreaming) might have tools to isolate and treat the compromised access port and obtain the details of the unauthorized access hacker as well as a tracer.

An example is plausibly the use of Backchannelling a new audible tones between resonance frequencies changes using traditional Morse code for packet switching and transportation. Another example could be rotating quantum qubits (magnets) as seen in Figure 1, type 'A' (clockwise—clockwise and clockwise—anticlockwise) then type 'B' (clockwise—anticlockwise and clockwise—clockwise). A Cypher example (traditional-Quantum) could be:

- Traditional packet switching (breaking up multiple path transmission-reassembling)
- Quantum packet slipstreaming (subspace scaffolding waves) is likely to have no intermediate nodes—cells only a unique entanglement to known property (resonance of a single entangled Atom P2P).
- Entanglement resonance may have an active sensor data as an outcome (e.g. data (sound) out of a number of speakers (magnets; diaphragm etc.)).
- Each sender—receiver may be based on multi entity (living—nonliving) communication history of disconformities to random radicals proprieties that may be used in a security key conceptualisation (Attachment 'B')

III. Method

Using Quantum bit (Qubit) entanglement properties (Figure 1) and a Morse code a new paradigm was developed. A feature was use of the properties as unique logic switches and algorithms of quantum qubit shuffling for a cypher code a cypher was proposed. Of particular interest are state changes from 'dot' (time unit 1) and 'dash' (time unit 3) to 'on' as one

(1) or 'off' as zero (0) for increased security by Backchannelling [22] [23] [27] [28] [29] [30].

IV. Data and Analysis

The data focused on the merging of various unique operational switches of quantum qubit shuffling. An output was a hybrid code called Quantum Morse code (Q-Morse) that can be utilises as Backchannelling to increase security of the active communications session. This suggests flux, field pattern and spectrum may be used as a cypher [22] [23] [27] [29] [30] as well as using the entanglement properties as a number of different types of logic gates function. These logic gates range from NOT, AND, OR, to XNOR (Exclusive NOR) combinations. An outcome desired is to achieve unique active sensing ('active perception of motion' (APMs)) and devices for improving secure Human–to–machines–to–entities (Biological; non–biological) and an inclusive 'Internet of Things' (IOT) ecosystem (Robotics 2050 vision) [31] [32] [33].

A. Quantum–Morse Code Cypher

Table 1 detail's the possible transition from Morse code to the utilization of the unique properties of the entangled Quantum bit (Qubit) to mitigate distortion—interdiction (Appendix 'A; and 'B') that can be Backchannelled to increase security.

TABLE I. Cypher using Quantum–Morse Code [22] to [30]

Example	Morse Code	Quantum (Cypher)		
		Digital	Entangled*	Flux
Alphabet				
A	.-	10	1001	Y
B	-…	0111	01111110	Y
Numeral				
0	-----	00000	0000000000	Y
1	.----	10000	1000000001	Y
Special				
Full stop	.-.-.-	101010	101010010101	Y
Comma	--..--	001100	001100001100	Y

*Properties include entanglement to flux changes and verification for Backchannelling (slipstreaming) using available Blockchains.

B. Subspace 'Quantum Subspace Communications' (QSC)

More secure messages in a congested spectrum might suggest use of a transfer node station within magnetic field wave (Fig 2) that is swarm like but can be directed. To assist the decision process consideration is given to 'causality logic gate delivery engines' that might be use (e.g. 'For-Bit Binary Add/Subtract Circuit' (FBBAS) to single multi input NAND Gate). An enabler might be a digital 'Radio Frequency' (RF) communication system using simplified Blockchains that are likely part of a 'Artificial Wisdom Intelligence' (AWI) that multiplex Backchannelling (slipstreaming) within and between various signal spectrum surface tensions [32] [33] [34] [35]?

Subspace communications could be like a Backchannelling (slipstreaming) Blockchain with a P2P mobile phone connection Backchannelling (slipstreaming). Logic gate type mixes (e.g. NOT, AND, OR, to XNOR) are likely swarm clusters that exists at the same time and n-dimensional space (before and after but making a communications interface). The superposition occurs for each unique sender and receiver and is not a prorogations wave (water drop in a puddle of water) but a directed Backchannelling (slipstreaming). Consider n-dimensional Hilbert space and Euclidean space as a hypercube (quantum entanglement-superposition) resonating within a specific spectrum and entangled quantum bit (Qubit) synchronised (asymptotically reduce parallel latency). The occurrences resonate in free space that may behave as a non-Newtonian fluid using quantum bit swarms to 'punch through' (Fig. 2) to enable entanglement, increased security and clarity of message via Backchannelling (slipstreaming).

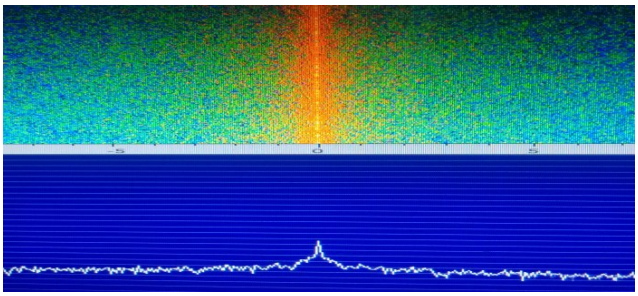


Fig. 2. 'Quantum Subspace Communications' (QSC) example encapsulates backchannelling (slipstreaming) logic gate swarms (Appendix 'A', 'B' and 'C') [15] [36]

The interface established should then be the gate-keeper to progressively audit (backchannelling the cypher and then uploaded clear text message and data to ensure that any attempted breech cannot cross reference external data semantics with the stored data. Continued communications of the decrypted message and date is still stored within an encrypted containment quantum bit directed swam (hive AWI mind?) and only trickled down with each compliant backchannelling audit report for continued 'Quantum Subspace Communications' (QSC) [16] [37] [38] [39].

C. Proposed Quantum cypher process

Within Attachment 'C" is the proposed Quantum properties based cypher example. It is a complex algorithm with 'one–time–keys' (OTK) that have short expiry times like some 'Rivest-Shamir-Adleman (RSA: signature; verification; encryption), Digital Signature Algorithm (DSA: signature; verification; decryption) and 'Elliptic Curve Digital Signature Algorithm' (ECDSA). The additional value lies in the use of trickled down with each compliant backchannelling audit report of secure encrypted private and public keys known as a 'Quantum Key Distribution' (QKD) leading to viewing of the trickled down plain text message and data. As Q–Morse is very simplistic the trickled down is predicated as extremely short.

Particular useability might be for robotics autonomies systems using 'Simultaneous Localization And Mapping' (SLAM) and 'Robot operating system' (ROS) that are in remote and difficulty communications conditions and susceptible to signal freaking-outs or operating ecosystems with congested spectrums or have high surrounding noises. The Quantum 'Signal-to-Noise Ratio' (SNR) is the indication of the

overall performance of signal processing (Transmitted Signal Power; to Received Signal Power).

The outcome sought related to additional layers of security using ongoing Backchannelling (slipstreamed) audits and verification keys during the communications session based on unique Quantum Blockchain typologies of the sender—receiver previous performances. Verification is ongoing through the current session by Backchannelling (slipstreaming) using available Blockchains (ongoing checks during session of: *authentication; user style; 'discontinuity of-service'; previous attempts of 'distributed denial-of-service' (DDoS); maintenance of 'end-to-end' (E2E) encryption; detection of sniffing as an intent of hacking event likely etc.*) [3] [4].

V. Finding

A. Interactions

By Backchannelling (slipstreaming) Quantum qubit shuffling (containment wave) in digital states for a new Morse code (Q–Morse) the 'Quantum Key Distribution' (QKD) uses directed and deliberate typology of logic gate swarms:

- Flux: Counterclockwise—anti–clockwise flux (state zero (0)), Clockwise flux (state one (1)).
- Wave propagation and patterning [29].
- Both states same time (zero (0) —one (1).
- Unique signal bands of each containment wave.
- Plausible Radio VLF–EHF spectrum hopping [29].
- Enables a cypher to be embedded to enhance security via a combination of flux (Up; Down), field pattern and spectrum [22] [23] [24] [27] [28] [29].
- Many random radial may occur in using a mix of biological and non-biological entities to further secure a specific message.
- Multiple keys may be enabled for initial authorisation and continued access to decoded message by backchannel (slipstreamed) ongoing decoding session verification keys that declare no interdiction by a 'man–in–the–middle' (MITM).
- Use of Multi entity (living—nonliving) communication conceptualisation (Attachment 'B').
- Need to have verification and Backchannelling (slipstreaming) using available Blockchains.

B. Communications

The act of communicating has artifacts that may be monitored and interdicted via Backchannelling (slipstreaming). It is an important consideration to understand and develop a profile ('method of operations' (MO)) that maps and patterns the unique active sensing ('active perception of motion' (APMs)) that encapsulates (Appendix 'A', 'B' and 'C') [29] [31] the 'Quantum Key Distribution' (QKD) to the typology of logic gate swarms relevant to the:

- sender,
- receiver;
- equipment (sensors; devices; peripheries);
- free space that the signal moves through for 'Quantum Subspace Communications' (QSC).
- Blockchain activity ledger history that is used in the single ongoing decoding session as an audit verification keys that can be used to predicted the expected sender—receiver properties and detected the hackers disconformities to random radicals.
- Backchannelling (slipstreamed) is plausible as a verification key(s) that may be based on sender—receiver haptic; biological and non biological properties as well as their disconformities to random radicals.

VI. Conclusions

Secure Quantum Morse code (Q–Morse) based communications may assist in additional security by backchannelling (slipstreaming) logic gate swarms relevant to the keys composed of living and non-living sensor and device ecosystem integration is plausible. Furthermore this could assist to drive an inclusive 'Internet of Everything' (IOE). Backchannelling (slipstreaming) quantum cyphers use multiple properties that could be unique to the entities. This tends to make hacking more difficult that traditional 'Rivest-Shamir-Adleman' (RSA), 'Digital Signature Algorithm' (DSA) or 'Elliptic Curve Digital Signature Algorithm' (ECDSA). Additionally quantum based backchannelling (slipstreaming) logic gate swarm keys may be set to detect out of scope variabilities suggesting probing sniffers.

Backchannelling (slipstreaming) the Blockchain data as a verification key(s) is plausible if quantum qubit shuffling (containment wave) scaffolding signals has digital states of 'Quantum Morse' (Q–Morse) code. The entangled states (e.g. Table 1: 'Full stop' (101010) entangled (101010010101)) with flux changes have the uniqueness to assign to either sender or receiver of both. Any uniqueness is used as check verification that the session is unlikely to have an unauthorized interdiction probing underway or inappropriate third party ('man–in–the–middle' (MITM)) manipulating data.

Another future opportunity is for the development of a Star Trek type subspace communications in congested signal spectrums or to a space probe on the edge of a galaxy. The subspace communications is likely to have unique 'Quantum Key Distribution' (QKD) based 'Supervisory Control and Data Acquisition' (SCADA) system [50] backchannelling (slipstreaming) logic gate swarms (Figure 2). Such a configuration might be developed using the typology of the communications system and user. This then facilitates secure slip streaming P2P packets with unique profiles of the sending—receiving system. Initially attempting to be contacted the receiver by the sender might be multiplexed to mitigate Quantum noise distortion (Appendix 'A', 'B' and 'C').

This means plausibility in using backchannelling (slipstreaming) logic gate swarms of Blockchain data as a verification key(s) (forwards—backwards) and activity is monitored on an ongoing base during the decoding session. Verification keys are Backchannelling (slipstreaming) is ongoing and updates the Blockchain during the session (e.g. train driver must incrementally activate a switch otherwise the train stops) using predicted—expected sender—receiver properties as well as their past history of disconformities to

random radicals encountered. In summary, Quantum Morse code (Q–Morse) plausibly is the enabler to additional security by Backchannelling (slipstreaming) during a communications translation session. Secondly Backchannelling (slipstreaming) allows robotic autonomies engineering, to seamlessly orientated and adaptable for both earth and space operations.

ACKNOWLEDGMENT

The author acknowledges the support of SCOTTYNCC Independent Research Scientists in the papers development.

REFERENCES

[01] D. Thomas; "ROS Introduction"; 2014; ROS org; http://wiki.ros.org/ROS/Introduction
[02] S. Riisgaard and M. R. Blas ; "SLAM for Dummies"; 2005; MIT Electrical Engineering and Computer Science; Massachusetts Institute of Technology; http://ocw.mit.edu/courses/aeronautics-and-astronautics/16-412j-cognitive-robotics-spring-2005/projects/1aslam_blas_repo.pdf
[03] M. DeCesare; "How massive DDoS attacks are undermining the Internet"; 2016; Crunch Network; AOL; https://techcrunch.com/2016/10/22/how-massive-ddos-attacks-are-undermining-the-internet/
[04] A. Moscaritolo; "Report Slams Snapchat, Skype Over Encryption"; 2016; PC Magazine ; Ziff Davis; PCMag Digital Group ; http://www.pcmag.com/news/348935/report-slams-snapchat-skype-over-encryption
[05] J. Lesurf; "Secret Codes and Cyphers"; 2006; University of St Andrews; https://www.st-andrews.ac.uk/~www_pa/Scots_Guide/info/.../codes/.../cyphers.html
[06]. G. A. Niblo; "Code Breaking "; 2015; National Cipher Challenge; University of Southampton; www.cipher.maths.soton.ac.uk/code-breaking
[07] SSH; "Key generation"; 2004; SSH Communications Security Corp ; https://support.ssh.com/manuals/client-user/40/key_generation.html
[08] A-K. A. Tamimi; "Performance Analysis of Data Encryption Algorithms"; 2006; CSE567M: Computer Systems Analysis (Fall 2006); Computer Science & Engineering; School of Engineering & applied Science; Washington University in St Louis; http://www.cs.wustl.edu/~jain/cse567-06/ftp/encryption_perf/
[09] CISCO; "Encrypt Pre-shared Keys in Cisco IOS Router Configuration Example"; 2006; CISCO; http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/46420-pre-sh-keys-ios-rtr-cfg.html
[10] E. Barker and A. Roginsky; " Recommendation for Cryptographic Key Generation "; 2012; NIST Special Publication 800-133; National Institute of Standards and Technology; U.S. Department of Commerce; http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133.pdf
[11] D. R. Cheriton; "SSH Public Key Authentication"; 2013; School of Computer Science; University of Waterloo; https://cs.uwaterloo.ca/cscf/howto/ssh/public_key/
[12] H-K. Lo; M. Curty; and K. Tamaki; "Secure Quantum Key Distribution"; 2015; Quantum Physics (quant-ph); Nature Photonics 8, 595-604 (2014); arxiv.org; Cornell University Library; https://arxiv.org/pdf/1505.05303.pdf
[13] R.L. Naik; P.C. Reddy and U.S. Kumar; " Provably Secure Quantum Key Distribution Protocols in 802.11 Wireless Networks "; 2011; International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 2 (6) , 2011, 2811-2815; http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.228.586&rep=rep1&type=pdf
[14] J.A. Ashiq*;* "Will Quantum Computers Threaten Modern Cryptography?"; 2015; Tripwire, Inc.; http://www.tripwire.com/state-of-security/featured/will-quantum-computers-threaten-modern-cryptography/
[15] A. Nordrum; "Quantum Computer Comes Closer to Cracking RSA Encryption";2016 ; IEEE Spectrum; http://spectrum.ieee.org/tech-talk/computing/hardware/encryptionbusting-quantum-computer-practices-factoring-in-scalable-fiveatom-experiment
[16] X. Xu; C. Pautasso; L. Zhu; V. Gramoli; A. Ponomarev; and S. Chen "The Blockchain as a Software Connector"; 2016; Data61's Trustworthy Systems Research Group (TS); *Commonwealth Scientific and Industrial Research Organisation* (*CSIRO*); https://ts.data61.csiro.au/publications/nictaabstracts/9244.pdf.
[17] C. Chappert, A. Fert and F. Nguyen Van Dau; "The emergence of spin electronics in data storage"; 2007; Macmillan Publishers Limited; Springer Nature; http://www.nature.com/nmat/journal/v6/n11/full/nmat2024.html
[17] Wikipedia (Ort), "Orthogonal frequency-division multiplexing", Wikimedia Foundation, Inc., 28 November 2014, http://en.wikipedia.org/wiki/Orthogonal_frequency-division_multiplexing.
[18] P. Rovillain, R. de Sousa, Y. Gallais, A. Sacuto, M. A. Méasson, D. Colson, A. Forget, M. Bibes, A. Barthélémy and M. Cazayous ; "Electric-field control of spin waves at room temperature in multiferroic $BiFeO_3$";2010; Macmillan Publishers Limited; Springer Nature; http://www.nature.com/nmat/journal/v9/n12/abs/nmat2899.html
[20] Wikipedia (Spi); "Spintronics"; 2016; Wikimedia Foundation, Inc.,; https://en.wikipedia.org/wiki/Spintronics
[21] J. Gregg; "Spin electronics"; 2016; Department of physics' Oxford Spintronics Group; University of Oxford; https://www2.physics.ox.ac.uk/research/spin-electronics
[22] F. Lichtman; "PopSci Q&A: Seth Lloyd Talks Quantum Computing and Quoogling"; 2011; http://www.popsci.com.au/science/popsci-qa-seth-lloyd-talks-quantum-computing-and-quoogling,376914
[23] S.L. Loyd; "Quantum Biology; Better Living Through Quantum mechanics"; 2014; http://www.pbs.org/wgbh/nova/blogs/physics/2014/03/quantum-life.
[24] I. J. Hampson and S. Hanssen; "Electrical trade principles – a practical approach"; 2009; Pearson Ed.
[25] A. Nicolosi; "Cybersecurity in a post-quantum world"; 2016; Schaefer School of Engineering & Science; NEXUS Research Magazine; Stevens Institute of technology; http://research.stevens.edu/post-quantum-cybersecurity
[26] Wikipedia (P2P) ; "Point-to-point_protocol_over_Ethernet"; 2016; Wikimedia Foundation, Inc.,; https://en.wikipedia.org/wiki/Point-to-point_protocol_over_Ethernet
[27] Wikipedia; "Morse code"; 2016; Wikimedia Foundation Inc.; https://en.wikipedia.org/wiki/Morse_code
[28] Handymariner; "Morse Code": 2016: Handy Mariner; www.handymariner.com
[29] A.R. Harish and M. Sachidananda; "Antennas and Wave Propagation"; 2014'' Oxford Uni Press.
[30] ACMA; "Morse Code Signals"; 2016; http://www.acma.gov.au/Industry/Spectrum/Radiocomms-licensing/Apparatus-licences/morse-code-signals.
[31] J.P. Rronczka; "Motion control in Environmental Biorheology using Inductance signal processing"; 2016; IEEE 2016 AMC 22 Apr to 24 Apr 2016 University of Auckland ; New Zealand.
[32] E. Coates; "Combinational Logic & Truth Tables"; 2016: Modula 22; Learn About Electronics http://www.learnabout-electronics.org/Digital/dig22.php;
[33] R. Bigwood; "Basic Logic Gates"; 2005; Department of Electronic Engineering; University of Surrey;; http://www.ee.surrey.ac.uk/Projects/CAL/digital-logic/gatesfunc
[34] E. Jonsson;"Exclusive OR/Exclusive NOR (XOR/XNOR)"; 2015; Lecture #6: More Complex Combinational Logic Circuits; School of Engineering and Computer Science; University of Yexas at Dallas; https://www.utdallas.edu/~dodge/EE2310/lec6.pdfgilent;
[35] Agilent, "Agilent Vector Signal Analysis Basics"; 2004; Application note 150-15; Agilent Technolohies; http://cp.literature.agilent.com/litweb/pdf/5989-1121EN.pdf
[36] Charles (HB0EGW), James (KA2RVO) and Jeffrey (WA6KBA); "Winrad"; 2010; original code by Alberto di Bene (I2PHD); Version 1.6.1 Build 116; Steinberg Media Technology GmbH
[37] L. Parsons; E. Haque and H. Liu; "Subspace clustering for high dimensional data: a review"; 2004**;** Volume 6 Issue 1, June 2004; ACM SIGKDD Explorations Newsletter ; ACM Digital Library; Association for Computing Machinery; http://dl.acm.org/citation.cfm?id=1007731.
[38] E. C. Carson, S. Williams, M. Lijewski, N. Knight, A. S. Almgren, J. Demmel, and B. Van Straalen; "Avoiding communication in geometric multigrid"; 2014; PMAA, Wednesday, July 2, 2014; Courant Institute of

Mathematical Sciences; New York University ; http://math.nyu.edu/~erinc/ppt/PMAASlides2014.pdf.
[39] Wikipedia (Sub); "Subspace"; 2016; Wikimedia Foundation, Inc.,; https://en.wikipedia.org/wiki/Technology_in_Star_Trek#Subspace.
[40] J. P. Ronczka, "Coalescence Theory–Strategic Management Planning in Australian ports", 2006; Australian Maritime College, Launceston, Tasmania.
[41] J. P. Ronczka, "Wisdom Open–System Semantic Identification (WOSSI) Mapping of Causality Logic Gates", 2009;WeST-2009
[42] J.P. Ronczka, "Bio-communications"*;* Participants presentation, 2015 RAS Summer School on Agricultural Robotics (SSAR), Australian Centre for Field Robotics, University of Sydney, (unpublished), 2015.
[43] P. Wilton, "8 things about Oxford's driverless tech", Oxford Mobile Robotics Group (MRG), Department of Engineering Science, University of Oxford, 2015, http://www.ox.ac.uk/news/science-blog/8-things-about-oxford%E2%80%99s-driverless-tech.
[44] N. Farsad; W. Guo and A. W. Eckford; "Tabletop Molecular Communication: Text Messages through Chemical Signals"; 2013; DOI: 10.1371/journal.pone.0082935; http://www.plosone.org/article/info%3Adoi%2F10.1371%2Fjournal.pone.0082935,
[45] H. M. Said; H. E. Hennawy; A. Eldain A. Omar and S. M. Kholaif; "LEA: Link Encryption Algorithm Proposed Stream Cipher Algorithm"; 2015; Volume 6, Issue 1, March 2015, Pages 57–65; Ain Shams Engineering Journal;_____Elsevier B.V ; Science Direct; http://www.sciencedirect.com/science/article/pii/S2090447914001051
[46] Wikipedia (Key); "Key cryptography"; 2016; Wikimedia Foundation, Inc.,; https://en.wikipedia.org/wiki/Key_%28cryptography%29
[47] P. V. Saraswathi and M. Venkatesulu ;" A Block Cipher Algorithm for Multimedia Content Protection with Random Substitution using Binary Tree Traversal"; 2012; Journal of Computer Science 8 (9): 1541-1546, 2012 ; College of Information Sciences and Technology ; CiteSeerX; Pennsylvania State University ; http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.686.652&rep=rep1&type=pdf
[48] IBM; "Comparison of IPv4 and IPv6"; 2016?; IBM Knowledge Center; https://www.ibm.com/support/knowledgecenter/ssw_i5_54/rzai2/rzai2compipv4ipv6.htm
[49] I P. Duffy; "Assignment of an Ethertype for IPv6 with LoWPAN Encapsulation"; 2016; IETF-Announce; Internet Engineering Task Force (IETF); https://datatracker.ietf.org/doc/draft-ietf-6lo-ethertype-request/
[50] P. Schavemaker and L. van den Sluis; "Electrical Power Essentials"; 2009; John Wiley & Sons, Ltd; Book: www.wileyeurope.com
[51] H. Ohno; "Impulsing Paradigm Change through Disruptive Technologies Program (ImPACT)"; 2016; Center for Spintronics Integrated SystemsTohoku University; http://www.csis.tohoku.ac.jp/english/overview.html/
[52] M. Rothenberg and J. King;" Social Uses of Communication Backchannels in a Shared Physical Environment"; 2006; School of Information; University of California at Berkeley; http://groups.ischool.berkeley.edu/backchannel/downloads/backchannel.pdf
[53] D. Heylen; "Computing backchannel distributions in multi-party conversations"; 2007; EmbodiedNLP '07 Proceedings of the Workshop on Embodied Language Processing; ; ACM Digital Library ; Association for Computing Machinery ; http://dl.acm.org/citation.cfm?id=1610065.1610068
[54] Wikipedia; "Backchannel"; 2016; Wikimedia Foundation, Inc.,; https://en.wikipedia.org/wiki/Backchannel
[55] K. Lambertz; "Back-channelling: the use of yeah and mm to portray engaged listenership "; 2011; Griffith Working Papers in Pragmatics and Intercultural Communication 4,1/2(2011), 11-18; **Griffith** University; https://www.griffith.edu.au/__data/assets/pdf_file/0005/384017/Lambertz-backchannelling.pdf
[56] A. Sullivan, S. Woolf,and J. Arkko; "Attacks Against the Architecture"; 2016; Chat Live IETF Community; Internet Engineering Task Force (IETF®); https://www.ietf.org/blog/2016/10/attack-against-the-architecture/

Attachment A
Artificial Wisdom Intelligence' (AWI) processes

[30] [31] [40] [41] [42] [43]

- **Foundation concepts:**
  - **Paradox influences: '**d*e Montaigne': 'nothing is so firmly believed as that which we least know'*
  - **C5I4:** These 'robotic' facilities use active sensing ('active perception of motion' (APMs)) devices–to–sensors. They might be deployed to support the C5I4 continuum ('Command—Control—Communications—Computers—Collaboration—Intelligence—Information—Integration—Interoperability')
  - **CPPWSRVC:** the sensor, an electromagnetic field is set up within the loop together with algorithms that 'calibrates—push—pull—wait—swap—recalibrate—verification—cascades' (CPPWSRVC)
  - **A6:** Biorheology soft robotics (Biobots) automated visual mapping could be applicable as 'anywhere—anytime—anyplace—anydevice—anycomms—anyentity' (A6).
  - **CSIANS:** ('calibration, synergy, integration, assimilation narrative and synchronization')
  - **PARRIFA:** 'Debt to be paid': 'portability—agility—redundancies—responsiveness—insight—foresight —adaptability' (PARRIFA)
  - **Wisdom open–system semantic identification**' (WOSSI) nexus of Critical path to Knowledge—information—learning threads as a 'Causality Logic gates' (COR gates) could be hybrid nucleus—kernels—control centres with Identified *'Wisdom abstraction virtual intelligence*' (WAVI) threads (some critical paths).
  - **'Causality Logic gates'** (COR gates) **via Coalescence theory** constructs as 'conjectures' (inferences):
    - **Coalescence theory:** *"entities, events; interactions—to—influences are interlinking continuums that are 'gooey–dough–like'"*
    - **Emerge**: *to come forth into view or notice*
    - **Stay**: *to spend some time in a place*
    - **Bonds:** *something that binds, fastens*
    - **Common:** *belonging equally to*
    - **Pivot**: *to turn about; rotate or oscillate*
    - **Changes**: *to make the form, nature*
    - **Decay:** *to decompose ; crumble*
- **Bio-plasma** Infusion; infiltration; exfiltration; shockwave
  - **Based on nexus:** *knowledge—information—learning delivery engines with hypercube/Hypersphere domains*
  - **Wisdom:** *judgment to plan a course of action*
  - **Causality:** *relationship between one event (called cause) and another event (called effect)*
- **Ackoff system of filters as 'conjectures' (inferences):**
  - **Information** ('who'; 'what'; 'where'; 'when'): *knowledge communicated*

- **Knowledge** (application of 'how'): *acquaintance with facts*
- **Understanding** (appreciation of 'why')**:** *comprehension process*
- **Wisdom** (evaluated 'why')**:** *judgment as to action; or insight*
- **Application** (Information; Knowledge; Understanding; Wisdom): *special use or purpose*
- **Appreciation** (Information; Knowledge; Understanding; Wisdom): *perception; recognition*
- **Evaluate** (Information; Knowledge; Understanding; Wisdom): *worth, or quality of; assess*

- **Delivery engine based:**
  - Complexities in the supporting knowledge—information—learning domains.
  - Outcomes tend to be false negatives, confusion, or skewed interpretation.
  - Process or series of processes that interact for a specific deliverable.
  - Set of predetermined protocols when an event occurs.
  - Unique trigger events, information—knowledge that has temporal meshing.

Conclusions:

- Appears to be cognitive predisposition to the way information and knowledge may be traditionally used.
- If critical constructs and associated domains are therefore skewed then compensators are required
- What may strengthen human—machine efficiency outcomes are system, threads and packets that have a 'Command—causalities—consequences' (C3) semantic modeling—dynamics
- A wisdom outcome for human—machine efficiency may be the coalescences of '*Command—communication—control*' of '*multiple—multiplexing—machines*' (C3M3) WOSSI delivery engines as radical drivers of not only uncertainty but achievable human—machine partnerships.

Attachment 'B'
Multi entity (living—nonliving) communication conceptualisation

Human—machine—bioentities (biobot insects) distributed communications and navigation [17] [18] [19]

Terms:

Biorheology logic gates, Metadata, Artificial wisdom intelligence; Informatics, multi–entanglements; Wisdom open–system semantic identification...

Introduction:

Broadly traditional communications may be suggested to align to verbal and non-verbal Semantic and Semiotic processes that align to:

- Transmitter, the receiver, and the channel [44].
- Communications may be an adaptation between the bioentity—machines—humans—interfaces.
- Capability 'anywhere—anytime—anyplace—anydevice—anycomms—anyentity' (A6).

Bio-communications:

They are Biosignals (signals of a biological entity (Bio-entity) that can be detected by another Bio-entity). The focus is on Biorheology in the context of bio-communications from Machine-to-Entities (M2E); Entities-to-Machine (E2M) and Entities-to-Entities (E2E). Robotic-to-Bio-entities (R2Be) communications has the potential to control crop pests in an environmentally sustainable way using a communications based intervention-countermeasure.

Tools:

The uses of:

- 'Artificial Wisdom Intelligence' (AWI) may be to embed them within a Bio-Kernel, Bio-logic gates or as Bio-Firmware.
- Biosignalling message stream as countermeasure—intervention to evasive entities (spoofing)?
- Firmware to software nudging.
- Wisdom open–system semantic identification (WOSSI).

Conclusion:

- Need 'Management—mitigation—mediation' (M3) of trans-entity-species C5I4 continuum domains and unintended consequences.
- Need detection of Chemistry—Biorheology signalling backbone packet Metadata to Big-Data; unintended consequences (cross talking entities).
- Need a focus on insect navaids complexity (Man in the middle; Hilbert space; Euclidean space; M space [Multiverse space]; 'de Montaigne' paradox).
- Outcome insect repurposing as a soft Robotic for Human good and Biocommunication (Biocomms) (magnetic field—frequency 'bubble' cascade).
- Nudging outcome: Transfer of hybrid Biocommunication (Biocomms) to robotic and soft Robotics based distributed C5I4 continuum ('Command—Control—Communications—Computers—Collaboration—Intelligence—Information— Integration—Interoperability') via navigation beacons with algorithms that 'calibrates—push—pull—wait—swap—recalibrate—verification—cascades' (CPPWS—R—C) as a continuum [41] [42].
- Backchannel (slipstreamed) verification keys based on sender—receiver haptic; biological and non biological properties disconformities to random radicals is plausible.
- The Entities communications interface appears to be bio-plasma membrane that is capable of infiltration—exfiltration data packets that are likely distributed hive mind collective able to undertaking extensive 'distributed denial-of-service' (DDoS) to negate 'end-to-end' (E2E) encryption as well as 'psychological operations electronic warfare' (Psy Ops EW) against the 'man–in–the–middle' (MITM) to force a change of thinking to negate the intended adverse actions?).

Attachment ‘C’
Proposed Quantum properties based cypher example

‘Challenge the present, drive the future’: Backchannel (slipstreamed) the Blockchain data as a verification key(s).

1: SENDER’S PLAIN TEXT (MESSAGE)

2: UNIQUE ENCRYPTING AND DECRYPTING KEY(S) DEVELOPMENT PROCESS [8 [45] [46] [47]**:**

2.1: Q–Morse

2.2: Flux

2.3: Frequencies

2.4: Entanglement

2.5: Wave scaffold

2.6: Slipstreaming (backchannel)

2.7: Mitigate distortion A (Atom—Molecule set properties)

2.8: Mitigate distortion B (Entities properties (haptic; bio-electrical; system configuration; power supply; Signal noise ration etc.)

2.9: Random radical detection and profiling (sender, receiver and system being used; uplink frequency; downlink frequency etc.)

2.10: Verification and Backchannelling (slipstreaming) during the communications session

3: ENCRYPTION (use Encrypting key(s)):

3.1: Cypher Key (Public: system entry) (>2048-bit’s)

3.2: Cypher Key (Private: entity specific e.g. credit card; PIN) (>2048-bit’s)

3.3: Cypher Key (Master: Biometrics; Body performance properties) (>2048-bit’s)

3.4: Verification of keys (Backchannelling (slipstreaming))

3.5: Check Security Strength of all keys (if non-compliant redo the algorithm process for another selection of keys)

4: ENCODED PLAIN TEXT (encrypted Sender’s Plain text message):

4.1: Verification Encoded Plain text (message)

4.2: Sent Encoded Plain text (message)

5: DECRYPTION (use Decryption key(s))**:**

5.1: Acquire decryption key(s)) (>2048-bit’s)

5.2: Apply decryption key(s)) (>2048-bit’s)

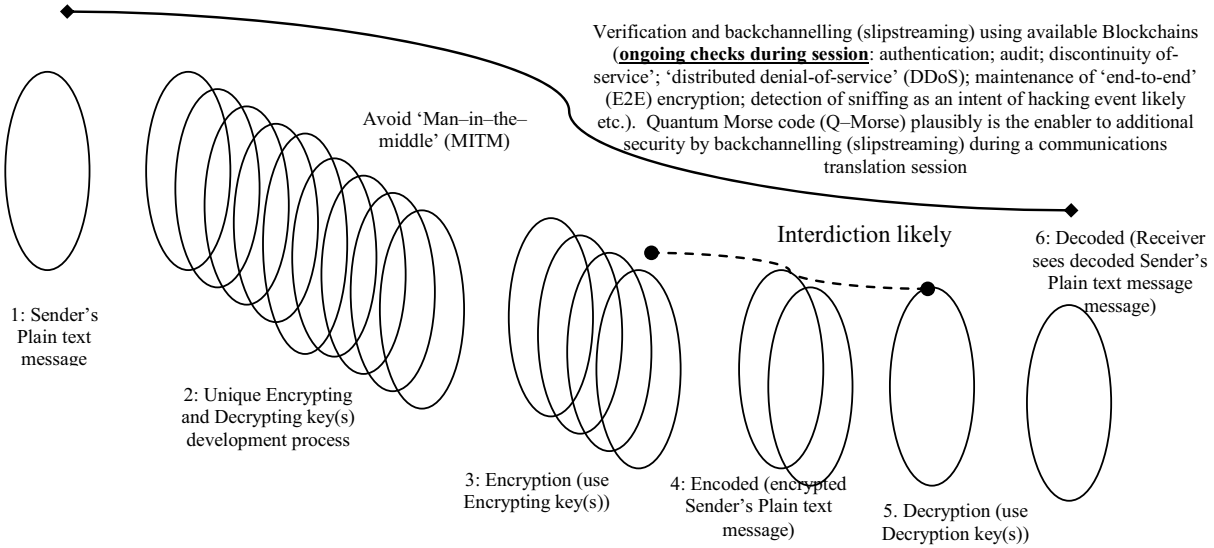
6: DECODED PLAIN TEXT (MESSAGE)

6.1: Receiver sees decoded Sender’s Plain text message

Note:
Notes:
1, **Security strength** score: if the key is say XXX bits long then expected to take about 2 x XXX operations to break [10].
2. **Verification** and Backchannelling (slipstreaming) using available Blockchains to check parameters during the communications session.
3. Cypher algorithm: See above, the emphasis is on the mitigation key and the need for the slipstream (backchannel) to complete the credibility nexus before decryption
4. **Cypher encryption decryption summary**

- **PROCESS**: **Plain text** (Message)… **Encryption** ….. **Cipher text** … **Decryption** ….. **Plain text** [8].
- Keys (shared key; private key) :
  - Symmetric Encryption (key algorithms) -same cypher sender-receiver ['A&B' agree on cypher system; 'A&B' agree on key used; 'A' encrypt using shared key; 'B' decrypt using shared key]; [8] [45] [46] [47].
  - Asymmetric Encryption (key algorithms) - different cypher sender-receiver ('A&B' agree on cypher system; agree on key used; 'B' sends its public key to 'A'; encrypts message using the negotiated cypher and 'B's' public key; 'B' decrypt the cyphered messages using its private key and the negotiated cypher) [8 [45] [46] [47].
  - Encryption…(block ciphers [ECB(Electronic Codebook Mode) clock cipher], which encrypt block of data of fixed size; stream ciphers [XOR function], which encrypt continuous streams of data (Link Encryption Algorithm (LEA: initial 128-bit key) is a word-oriented (parts: driving; combining) using Linear Feedback Shift Registers (LFSRs))…… authentication mechanism [8 [45] [46] [47]
  - Cypher (algorithm [steps involved; mathematics) security functions bundle for secrecy of message goals [8 [45] [46] [47]
- ***Authentication:*** identity verified [8 [45] [46] [47].
- ***Secrecy or Confidentiality:*** authenticated OK to interpret message [8 [45] [46] [47].
- ***Integrity:*** Integrity check sum of packet in address by IPv4 (nnn.nnn.nnn.nnn,) now IPv6 (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx) packets [48] [49].
- ***Non-Repudiation:*** neither falsely deny message [8 [45] [46] [47].
- ***Service Reliability and Availability:*** grant intended users required quality of service (QOS) [8 [45] [46] [47].
- ***Mode of Operations***: CTR (counter), CFB (Cypher Feedback), or DES (specific modes: ECB; CBC) [8]
- ***Logical:*** character sequence (long period; nonlinear) building key; complex mathematically [8 [45] [46] [47].
- ***Interdiction minimised:*** Quantum computer contradiction as 'Rivest-Shamir-Adleman (RSA) keys of 2048-bit likely broken by 100 million gates and 4000 qubits. There is a liability by using longer key lengths in terms of the systems performance. The system administrator has a dilemma in balancing the security level with the system quality of service (QOS). [8] [11] [14]
- ***Complexity of Keys****:* Be Asymmetric (minimum 2 keys) not Symmetric (single key); Public key (encryption); Private key (decryption ; must be very difficult to break) ; A Master key (all keys encrypted again) might be used on the Public and Private Keys as an additional security layer (encryption; password (decryption)) [7] [9] [11] [46]
- ***Spooling*** (like a sail sheet winding tightly) scaffolding of signal packets to establishing a quantum wave to access a nexus (circular shape with a number of small injection aperture—antenna) used in a prescribed cycle to deliver micro signal entanglements. The process may be multiple injection cycles in a circle to establish quantum scaffolding (entangled periphery swarms of nano signals) for subspace communication.
- ***C5I4 focus***: 'Supervisory Control and Data Acquisition' (SCADA) system for verification and Backchannelling (slipstreaming) using available Blockchains (**ongoing checks during session**: authentication; audit etc.) [50].\
- ***Spinmechatronics*** structures based on transistors for magnetic–tunneling layer stacking to spin waves (magnonic; polarized; cycloidal; frequencies than can be turned) develop a more secure, environmentally friendly and sustainable sensors and devices [17] [18] [51],

Cypher based on Quantum bit (qubit) 'shuffling' spooling Algorithm



Notes:
1: The traditional concept of Backchannelling has ranged from instant messaging in social networks (e.g., fact-checking; Skye to Twitter).
2. In the 'Artificial Intelligence' (AI) and 'Artificial Wisdom Intelligence' (AWI) context it refers to the AI/AWI secretly checking compliance of the hardware and software to ensure they are not compromised.
3. There is a need to consider new paradigms due to the recent large scale 'Distributed Denial of service' (DDOS) involving misconfigured to compromised nodes and associated old devices with very poor security process that cascade a large scale event that should have been foreseen [30] [31] [40] [41] [42] [43] [52] [53] [54] [55] [56].