Cryptology ePrint Archive: Report 2019/913

Information Conservational Security with "Black Hole" Keypad Compression and Scalable One-Time Pad—A Quantum Intelligence Approach to Pre- and Post-Quantum Cryptography

Wen-Ran Zhang
Department of Computer Science
Georgia Southern University, Statesboro, GA USA
(wrzhang@georgiasouthern.edu)

ABSTRACT— ABSTRACT—Whereas it is widely deemed impossible to overcome the information theoretic optimality of the one-time pad (OTP) cipher in pre- and post-quantum cryptography, this work shows that the optimality of information theoretic security (ITS) of OTP is paradoxical from the perspective of information conservational computing and cryptography. To prove this point, ITS of OTP is extended to information conservational security (ICS) of scalable one-time pad (S-OTP) where total key length can be compressed to a condensed tiny minimum through "black hole" keypad compression coupled with "big bang" data recovery. Thus, ICS/S-OTP makes it possible for secure transmission of long messages that used to be impossible with ITS/OTP. It is proven that if ITS/OTP is optimal, ICS/S-OTP would be impossible; on the other hand, if ICS/S-OTP is not information theoretically secure, ITS/OTP would not be secure either. Thus, we have a proof by contradiction on the paradoxical nature of OTP optimality. It is further proven that a summation with percentage distribution is a special case of equilibrium-based bipolar quantum cellular automata. This proof bridges a classical world with a quantum world and makes it possible to combine the advantages of both approaches for pre- and post-quantum cryptography. It is suggested that the findings of this work form an analytical paradigm of quantum intelligence machinery toward perfect information conservational security. Some mysteries in nature and science are identified and discussed. In particular, the question is posted: Could modern science have been like a well-founded building with a floor of observable beings and truths but missing its roof for equilibrium, harmony, information conservation, and logically definable causality?

KEYWORDS: Pre- and Post-Quantum Cryptography; Scalable One-Time Pad; Information Conservational Security (ICS); "Black Hole" Keypad Compression; "Big Bang" Data Recovery; Collective Precision; Quantum Intelligence; Classical World; Quantum World; Floor-Roof Mysteries

1 INTRODUCTION

Cryptography is essential for the security of digital communication. However, many commonly used cryptosystems could be completely broken by a *quantum* algorithm for integer *factorization [1]* once large quantum computers are commercially applicable. Post-quantum cryptography is to counter such quantum attacks and to keep digital communication secure *[2]*. A key for success is to identify mathematical operations for which quantum algorithms offer little advantage in speed, and then to build cryptographic systems around them.

One-Time Pad (OTP) is often regarded the only cipher with proven information theoretic security (ITS) *[3]* for cryptography. ITS derives security from information theory *[4]*. It was introduced in 1949 by American mathematician Claude Shannon—the inventor of information theory, who used it to prove the optimality of OTP in security *[3]*. Since then, OTP has been used for the most sensitive communications. It can now be used together with quantum key distribution (QKD) — a well-developed application of quantum cryptography.

Since OTP is quantum proof to quantum factorization *[1]*, it is often regarded the only candidate for post-quantum cryptography as well *[2]*. Unfortunately, the key requirement of equal or greater length than the original message hinders the general application of OTP. As a result, OTP is so far limited to transmitting relatively short messages with high security requirement. This limitation has been an impasse for both pre- and post-quantum cryptography. A major challenge is therefore to reduce the OTP key length without weakening ITS where the gain of key length reduction significantly overweighs its cost.

This work extends ITS of OTP to information conservational security (ICS) of Scalable One-Time Pad (S-OTP) with a quantum intelligence approach. In this approach, an S-OTP cipher does not attempt to falsify Shannon's theorem on OTP. Instead, it gets around the problem by proving the paradoxical nature of the ITS optimality of OTP through a proof by contradiction. Then, with "black hole" keypad compression it reduces OTP key length to a tiny minimum and makes the transmission of long messages systematic and practical without weakening ITS in its new context.

It is further proven that a summation with percentage distribution is a special/minimum case of equilibrium-based bipolar quantum cellular automata. This proof bridges a classical world with a quantum world and makes it possible to combine the advantages of both approaches for pre- and post-quantum cryptography.

It is suggested that the findings of this work form an analytical paradigm of quantum intelligence toward perfect information conservational security. Some mysteries in nature and science are identified and discussed. In particular, the question is posted: *Could modern science have been like a well-founded building with a floor of observable beings and truths but missing its roof for equilibrium, harmony, information conservation, and logically definable causality?*

Following this introduction, the remaining work is organized in four sections: an axiomatic formulation, a methodological formulation with illustrations, a quantum architecture, and some conclusions. (Note: Some similar concepts of ICS are proposed in an unpublished technical report on a failed attempt *[5]*. This work is built upon the failure. The failed attempt is further compared in the next section.)

2 AXIOMATIZATION

An OTP cipher is proven information theoretically secure and unbreakable *[3,4]* provided that the cipher key meets the four conditions of OTP*:* (a) truly random; (b) never reused; (c) kept secret from all possible attackers; (d) of equal or greater length than the message. History shows that, however, when Shannon invented information theory and ITS *[3,4]*, the first computer was not out yet. Since then, computing theory and technology have advanced beyond anyone's imagination. Although it was proven *[3]* that any cipher with the perfect secrecy property must use keys with effectively the same requirements as OTP keys, these proofs did not take later computing theories and technological development into consideration that can conceal the meaning of a message. For instance, when entropy became a key concept in information theory, information conservational computing/cryptography (ICC) as an analytical model for quantum intelligence (QI) *[6,7]* was not incepted yet. Furthermore, before the first computer was put on drawing board, double-precision floating-point format for a wide dynamic range of numeric values was unimaginable. The wide range makes equilibrium-based ICC practical where a unit value 1 can be virtually composed of an infinite number of different fractions to form a basis for information conservation. Thus, ICC with QI is different from big prime integer factorization with a finite space of solutions *[1]*, different from ITS, and different from classical information theory.

Entropy as a measure of disorder of a system provides a basis for classical information theory. Based on entropy unicity distance *[3]* is defined as the minimum amount of ciphertext required to permit a computationally unlimited adversary to recover the unique encryption key in a brute force attack.

The ICC extension, however, attempts to incorporate holistic and set-theoretic keypad compression into S-OTP as an analytical quantum-digital compatible extension to ITS with

QI including bipolar equilibrium-based rebalancing, collective precision, "black hole" keypad compression, "big bang" data recovery, logically definable causality, quantum entanglement, quantum teleportation, classical world, and quantum world.

Axiom 1. Within computational precision limitation, the plaintext L of any OTP message in binary format can be divided into a set of N integers $\{x_i\}$, $1 \le i \le N$, such that the pair $(X, \{x_i/X\})$ conserves the information of L, where $X = \sum_i x_i$ is referred to as a *virtual summation*, and $\{x_i/X\}$ a *virtual percentage distribution*.

Axiom 2. While the OTP cipher conceals the semantics of text data for ITS based on entropy, an information conservational extension does not have to be strictly based on entropy because the pair $(X, \{x_i/X\})$ in Axiom 1 does not show original semantics of the plaintext regardless of the entropy measure of its key pad.

Hypothesis. The pair $(X, \{x_i/X\})$ can be secured without using a greater or same length keypad as required by the OTP cipher for ITS based on Shannon entropy, and a key can be reused in securing part of the percentage distribution $\{x_i/X\}$ under certain conditions.

Definition 1. *Information conservational transformation (ICT)* is referred to as a set of set-theoretic mathematical functions that form a transformation T to transform the bit pattern of a long message in form F_1 to a pair of (F_2,F_3) such that there is a reverse transformation T' that recovers F_1 from the pair (F_2,F_3). Formally we have: $T(F_1)$: $F_1 \rightarrow (F_2,F_3)$, such that $\exists$T' and T'(F_2,F_3): $(F_2,F_3) \rightarrow F_1$. F_2 is assumed an integer summation $X = \sum_i x_i$, and F_3 a percentage distribution $\{x_i/X\}$. Thus, F_2 is significantly shorter than F_1, and F_3 longer than F_1 with a limited data length increase.

Definition 2. *Scalability* is referred to as using ICT once or multiple times systematically to transform a long message or large data set in form F_1 into (F_2,F_3) such that the total OTP cipher key length is reduced to a condensed minimum for secure transmission of the (F_2,F_3) pair. In this case, a cipher is referred to as *Scalable OTP (S-OTP)*, and classical OTP is referred to as *Virtually Scalable OTP* or *VS-OTP*.

Definition 3. S-OTP is said having *information conservational security (ICS)* provided that: (a) The total key length required is significantly shorter than the original message due to ICT; (b) The shorter key does not weaken the ITS of OTP in terms of OTP being VS-OTP; (c) The gain significantly overweighs the cost.

Definition 4. *"Black Hole" Keypad Compression (BHKC)* is referred to as total keypad length reduction for long messages that compresses the keypad to a condensed tiny minimum through a hierarchy of ICTs; *"Big Bang" Data Recovery (BBDR)* is referred to as the reverse process of BHKC.

It could be argued that S-OTP is just OTP plus data compression, and there is nothing new. The reality is:

- *Energy/Information conservation or preservation as a paramount law in modern science and ICC as a long sought goal in physics and information theory has been computationally unreachable;*
- *The keypad length requirement of ITS/OTP has been a longstanding impasse;*
- *ICS/S-OTP only reduces keypad length but not total data length. It actually costs a limited data traffic increase—a guarantee of no information or entropy loss.*
- *ICS could, if proved, contradict the ITS optimality of OTP for the first time ever;*
- *ICS could be proven a holistic extension to ITS with a higher level of abstraction;*
- *ICS could be extendable to quantum-digital compatible computing and cryptography machinery.*

The inception of ICS accounts for the new development in computing technology. Double precision floating-point format of IEEE binary128 is used as a technological basis in this work that was not available when information theory was initially developed based on Shannon entropy *[4]*.

Basic Cost-Gain Analysis. Let each 1K-bit data divided into ten 96-bit sections plus one 64-bit section, total $1K=960+64=1024=2^{10}$ bits. L=32K bits would be divided into 320 of 96-bit sections plus 32 of 64-bit sections, a set of 352 integers $\{x_i\}$, $1 \le i \le 352$. The summation of all integers is smaller than $96+9=105$ bits because $352 < 2^9$. Based on IEEE binary128 standard with 112 significant bits precision and 16-bits exponent, we would have

one integer summation $X = \sum_i x_i$ with no more than 105 bits (<112) and a set of 352 percentages $\{x_i/X\}$ in double precision floating-point format, each has 128-bits. While an OTP key requires the minimum length of 32K bits that is the message length. Without computational precision problem, an S-OTP key could potentially be compressed to the length of the 105-bit summation in 128-bit double precision floating-point format, a 32K/128 = $2^{15}/2^7$ = 256-fold key length reduction. Assuming more room is given to the S-OTP key for partial concealment of the percentage distribution after they are used to encrypt other percentages, we could have:

(1) For a 1K-bit key, the saving would be 32K/1K=32-fold;
(2) For a 2K-bit key, the saving would be 32K/2K=16-fold;
(3) For a 4K-bit key, the saving would be 32K/4K=8-fold;
(4) For an 8K-bit key, the saving would be 32K/8K=4-fold.

The summation and the percentage distribution total data length approximates to 128 + 352 × 128 bits ≈ 44K bits for the 32K-bit message. The cost is roughly a (44-32)/32 = 12/32 =3/8 = 37.5% increase in data length and network traffic. The gain could include (i) to make the transmission of long messages possible; (ii) to reduce the cost of quantum key distribution by 32K/2K = 16 folds. Evidently, the gain significantly overweighs the cost.

It should be remarked that the failed approach reported in *[5]* also attempted to secure a summation and a percentage distribution. While both are aimed at information conservation, the former attempted to compress the whole plaintext to a condensed tiny minimum and was proven impossible due to the loss of information or entropy. The latter is focused on compressing the keypad only with a limited network traffic increase as a tradeoff.

Theorem 1 (Security Theorem). ICS of S-OTP does not weaken the ITS of OTP provided that (a) summation $X = \sum_i x_i$ is enciphered with a same length or longer private S-OTP key equivalent to an OTP key, and (b) the percentage distribution $\{x_i/X\}$ is made completely misleading and uncorrectable without private key.

Proof. *If the percentage distribution is completely misleading and uncorrectable by an attacker in a brute force attack, the plaintext concealed in the ciphertext of a summation is safe. On the other hand, without the key to the summation, to find a correct percentage through trial and error for revealing the plaintext would be as difficult as finding a virtual percentage to reveal a section of the plaintext of an OTP message in a virtual summation per Axioms 1 and 2. This leads to a proof by contradiction. Under the two conditions, if an attacker could still find a percentage to reveal the plaintext of a data section in S-OTP ciphertext, it would be possible to do it similarly to reveal the plaintext of a data section of any OTP ciphertext and its virtual summation. If this could really happen, OTP as VS-OTP would be made irrelevant by S-OTP because entropy and unicity distance would be bypassed. That would contradict not only the optimality of OTP but also the ITS of OTP.* ■

Theorem 2 (Optimality Theorem). If OTP is information theoretically secure, S-OTP must be information theoretically secure under the two conditions of Theorem 1. However, if S-OTP is information conservationally secure, OTP is not information theoretically optimal.

Proof. *S-OTP is information theoretically secure per Theorem 1 under two conditions. However, if S-OTP were information-theoretically secure, OTP would not be information theoretically optimal because its key length could be scaled down using ICS with a limited data overhead for a benefit that significantly overweighs its cost.* ■

Theorem 3 (Security Level Theorem). ICS is a holistic top-down approach to information security at a higher level of abstraction than ITS—a bottom-up approach strictly based on entropy and unicity distance. This difference makes it possible for partial reuse of an encryption key in S-OTP that does not have to be strictly based on entropy.

Proof. *Since an S-OTP cipher is to conceal a summation and a percentage distribution without plaintext semantics, it is different from an OTP cipher but more general. While plaintext can be revealed based on semantics due to low entropy of an OTP key, summation and percentage distribution do not show such semantics. A guessed percentage in a trial cannot be confirmed without its key or a confirmed summation plus a confirmed distribution; a guessed summation cannot be confirmed without its key or a confirmed distribution*

plus deterministic semantic analysis. Thus, ICS of S-OTP is a fundamentally different approach that does not have to be strictly based on entropy as for ITS of OTP. After all, OTP is VS-OTP, and information conservation is a paramount law in modern science. Entropy, on the other hand, is information but not a law. ■

3 METHODOLOGY

3.1 Basic ICC Algorithm

The rationale of S-OTP is that, given an unsigned big integer L representing large data item D to be transmitted, L can be divided into a set of short integers $\{x_i\} = \{x_1, x_2, .., x_i, .. x_N\}$ representing sections of D to be transmitted. The math summation can be obtained as $X = \sum_i x_i$, $1 \le i \le N$, which is concealed in the ciphertext of key K_1 in the same way as using an OTP key. The ciphertext of X is much shorter than L to transmit. The percentage distribution $\{x_i/X\}$ can be longer than L but it can be made completely misleading with K_1 indirectly. While part of the distribution can be concealed together with the summation using K_1, the concealed percentages can be used for as encryption keys for the other part of the percentage distribution. For instance, P terms of the percentages can be partially concealed with K_1 together with the summation, and the remaining $(N - P)$ percentages $\{x_i/X\}$ could be encrypted using three 128-bit short private keys. If we assume the data sections are random and so the partially concealed percentages, the three short keys can be replaced with three partially concealed percentages. Let p_1, p_2, and p_3 be the maximum, median, and mean (max-median-mean) values of partially concealed percentages, we have the 2-layer encryption defined in Eq. 1.

$$\forall i,\ P<i\le N \text{ and } (i\%2) = 0,\ \{\boldsymbol{x_i/X}\}' = \{[p_1 + (\boldsymbol{x_i/X})] \,/\, [\mathbf{1} + \mathbf{0.5}\boldsymbol{N}(p_1 + (\boldsymbol{x_i/X}))]\}\ ; \quad \textbf{(1a)}$$

$$\forall i,\ P<i\le N \text{ and } (i\%2) = 1,\ \{\boldsymbol{x_i/X}\}' = \{[p_2 + (\boldsymbol{x_i/X})] \,/\, [\mathbf{1} + \mathbf{0.5}\boldsymbol{N}(p_2 + (\boldsymbol{x_i/X}))]\}\ ; \quad \textbf{(1b)}$$

$$\forall i,\ P<i\le N,\quad \{\boldsymbol{x_i/X}\}'' = \{[p_3 + (\boldsymbol{x_i/X})'] \,/\, [\mathbf{1} + \mathbf{0.5}\boldsymbol{N}(p_3 + (\boldsymbol{x_i/X})')]\}\ . \quad \textbf{(1c)}$$

Eq. 1 assumes: (a) $(\boldsymbol{x_i/X})$ and p_i are a random percentages non-linearly correlated with each other; (b) Integers P and N are private until the receiver count the number of concealed percentages by K_1. With the two conditions there is no common factor involved even though p_i and N are reused. Thus, Eq. 1 is quantum proof to factorization.

Preprocessing. This work assumes that the data sections of the plaintext to be enciphered is random without zero sections. The assumption is reasonable because such sections can be categorically compressed.

Theorem 4 (Possibility Theorem). A partial percentage distribution can be made completely misleading with Eq. 1 and uncorrectable by an attacker without any private key.

Proof. *The task of Eq. 1 is to make a partial percentage distribution misleading and uncorrectable by an attacker without private key where the distribution does not have to remain rational. The theorem follows from six conditions. First, Eq. 1 has no common factor due to the non-linear correlation of p_i and (x_i/X) in multiple layers. Second, with private key obtained from QKD K_1 is really random. Third, with complete concealment of the summation and partial percentage distribution, the remaining part of the distribution does not sum to 1.0 and no longer correlated. Fourth, applying Eq. 1 with the max-median-mean values in double layers conceals the remaining percentages completely and makes them uncorrectable. Fifth, data preprocessing guarantees that no zero data section. Sixth, different pieces of encrypted data are isolated and interlocked with information conservation. A guessed key p_i in a trial cannot be confirmed until the encrypted percentage is confirmed; a guessed percentage distribution cannot be confirmed without being tested against a confirmed summation; a guessed summation cannot be confirmed without its key or a percentage distribution plus deterministic semantic analysis which is generally non-deterministic. Thus, the only option is exhaustive search.* ■

The total S-OTP key K_1 for enciphering the summation plus P terms of the percentages could have (128 + 128P) = 128(1+P) bits. Assuming a 32K-bit data length we have the comparison between S-OTP and OTP: (i) Let P = 7, the key length 128(1+P) approximates to 1K bits with 32-fold key reduction. (ii) Let P = 15, the key is about 2K bits with 16-fold key reduction. (iii) Let P = 31, the key is about 4K bits with 8-fold key reduction. (iv) Let

P = 63, the key is about 8K bits with 4-fold key reduction. (v) Let P = 127, the key is about 16K bits with 2-fold key reduction.

S-OTP-Method1

Assume IEEE binary128 is used within the limit of computational precision, and sender Alice and receiver Bob share private key K_1 distributed through QKD. $\forall i, x_i>0$.

Part I. Encryption

Step 1. *Let $\{x_i\}$ represent preprocessed data sections;*

Step 2. *Let math summation $X = \sum_i x_i$, for all i (not XOR);*

Step 3. *Calculate percentage distribution $\{x_i/X\}$;*

Step 4. *Encrypt X and P terms of $\{x_i/X\}$ with key K_1 to X'=[$K_1 \oplus$(X concatenates P terms of x_i/X)] where $\oplus$ is XOR (not math summation); apply Eq. 1 to encrypt the remaining terms of $\{x_i/X\}$ to $\{x_i/X\}$";*

Step 5. *Alice Transmits E = (X', $\{x_i/X\}$") to Bob as a pair.*

Part II. Decryption

Step 1. *Use K_1 and Eq. 1 to decipher or decrypt E to the pair (X, $\{x_i/X\}$);*

Step 2. *Use $\{x_i/X\}$ to decrypt the summation X to $\{x_i\}$;*

Step 3. *Recover the message from $\{x_i\}$ with concatenation.*

Example. Assuming the plaintext data *D* to be transmitted is represented by *L = 1048549998213983988* divided into the three sections *1048549, 998213, and 983988.* Assume sender Alice and receiver Bob share key K_1.

Part I – Encryption (some steps are omitted)

- *Let x_1 =1048549, x_2 = 998213, x_3 = 983988; X = $x_1 + x_2 + x_3$= 3030750;*
- *Calculate percentage distribution $\{x_i/X\}$ = {34.5970%, 32.9362%, 32.4668%};*
- *Encrypt and transmit;*

Part II – Decryption (some steps are omitted):

- *Use K_1 and Eq. 1 to decrypt the message;*
- *U=(3030750, {34.5970%, 32.9362%, 32.4668%});*
- *Recover x_1 = 1048549, x_2 = 998213, and x_3 = 983988;*
- *L = concatenate(x_1, x_2, x_3) = 1048549998213983988;*
- *Recover D from L.*

Theorem 5. S-OTP-Method1 is information conservationally secure provided that Theorem 4 holds.

Proof. *The conditions of ICS are met: (a) The key length required is significantly shorter than the message due to ICT. (b) The shorter key does not weaken the ITS of OTP being VS-OTP because the summation is enciphered with an S-OTP key equivalent to an OTP key, percentage distribution is partially concealed, and remaining percentages are made completely misleading and uncorrectable without the key per Theorem 4. (c) The gain of many-fold key reduction significantly overweighs the cost—a limited data traffic increase of 37.5% countered by a 4- to 32-fold reduction of key length and key distribution cost to make it possible for safe transmission of long messages.* ■

It is undoubtedly a big step to advance from ITS/OTP to ICS/S-OTP. While ITS/OTP takes a bottom-up approach to cryptography, ICS/S-OTP takes a top-down approach. One is probabilistic and another holistic. One is observational and another information conservational. One is statistical and another logical. Notably, the plaintext in S-OTP is holistically transformed into isolated but interlocked and meaningless little pieces whose complete correlation cannot be revealed until the plaintexts of all pieces are revealed with keys. It is understandable that this leads to doubts and confusions that deserve further clarification.

Clarification 1. It can be argued that, since S-OTP exposes the approximate number of data sections, it cannot be compared with OTP where the plaintext is enciphered with a same length or longer keypad based. This is an invalid argument. A same length key exposes the exact data length while a longer keypad exposes the approximate data length.

Clarification 2. It can be argued that the S-OTP idea is quite similar to the already well-researched key stretching technology *[8]*. This is an interesting observation where an enhanced or stretched key should be of sufficient size such as 128 bits to make it infeasible

to break by a brute force attacks. Notably, a 2K-bit or longer integer key and 128-bit decimal keys are used in S-OTP as well. It seems similar, however, a fundamental difference is information conservation. With ICS/S-OTP, key K_1 without reuse conceals a summation and part of the percentage distribution in the same way as an OTP key does with ITS; private keys or the max-median-mean values of partially concealed percentages can be used as reusable keys to encrypt the remaining percentages. The 128-bit keys and the encrypted percentages are both in double precision floating-point format. Since the summation and percentage distribution are resulted from ICT, no semantics of bare plaintext is involved. While a guessed password can be readily tested in a trial, a decimal key for a percentage cannot be confirmed until the encrypted percentage and the entire distribution is confirmed. A percentage distribution cannot be confirmed without being tested against a confirmed summation. A guessed summation cannot be confirmed without its key or a confirmed percentage distribution. Thus, the isolated and meaningless little pieces are interlocked that have to be semantically revealed holistically either with a key or exhaustive search.

Assuming a 2K-bit key K_1 and 128-bit fixed-point decimal format keys for percentages, the search space for K_1, p_1, p_2, p_3 , and N could be estimated as $SP = 2^{2048} \times 2^{128} \times 2^{128} \times 2^{N}$. Given N = 352, SP = 2^{2656}. It seems a deterministic search space. Unfortunately, fixed-point format is far from sufficient for double precision floating-point computing. Moreover, without the key, S-OTP would require a brute force attack to perform semantic analysis that is generally non-deterministic in nature. Thus, S-OTP looks similar but fundamentally different from key stretching that must have a deterministic space such as 2^{128}.

It should be pointed out, however, since the summation and percentage distribution can be deemed attributes, the use of partially concealed percentages as keys in ICS/S-OTP can be deemed an information conservational extension to attributed-based privacy *[9,10,11]*. It extends attribute-based asymmetric privacy for data sharing to a symmetric key protocol for general-purpose cryptography. The technique can be named as *percentage-based information conservational key extension (PBICKE).*

Clarification 3. Yet another major argument is that using an S-OTP key to encrypt a long message to reach ITS requires the min-entropy of the S-OTP key to be the same as OTP key, and the length of S-OTP key must be equal or larger than the length of the OTP key. Thus, it is impossible for the ICS of S-OTP not to weaken the ITS of OTP for long messages, and Definition 3 has to be wrong.

A counter argument to the critique seems difficult but readily lies in the context of OTP being VS-OTP. Based on Axioms 1-2 and Definitions 1-4, OTP is virtually scalable where any plaintext message can have a virtual summation with a virtual percentage distribution. This leads to the paradoxical nature of the ITS optimality of OTP (see Theorems 1-4) because, for the first time, a computationally unlimited adversary can guess a virtual percentage and a virtual summation with a trial and error method regardless of any entropy measure of the OTP cipher key. Thus, if an adversary can be forced to bypass an S-OTP key to guess a percentage and a summation, the adversary can also bypass an OTP key to guess a virtual percentage and summation. ITS/OTP has to face this newly discovered reality where some conventional concept is no longer classical.

Subsequently, we can conclude that S-OTP does not weaken the ITS of OTP as long as the two security conditions of Theorem 1 are met no matter whether ITS in its new context is stronger, weaker, or same as before (a topic left for future study). Our focus then should be on the two security conditions with: (a) holistic information conservation, (b) semantic information hiding, (c) summation isolation from percentage distribution, (d) partitioning and concealing the percentage distribution, and (e) key pad compression with collective precision. While Shannon entropy is used as a basis, other entropy measures are left for future research effort for possible enhancement.

3.2 ICC with Collective Precision

S-OTP-Method1 with percentage distribution has its limitation in computational precision and data traffic overhead. When the math summation gets huge—a usual case, the

precision of a single percentage is problematic. The 37.5% data traffic increase is also a significant factor. These problems can be better solved with the massive parallel collective precision property of ICC *[6,7]*. In ICC, a big integer total can be divided into many subtotals of different data sections. If each subtotal is further divided into bipolar import and export, each can be normalized by its corresponding column subtotal. An information conservational matrix can then be derived through column-major normalization for parallel and collective precision without using a grand total.

Without dealing with the grand total, a section subtotal can be increased to reduce the number of sections as well as percentages and data traffic overhead. For instance, section size can be increased from 96 bits (12 bytes) to a maximum 112 bits (14 bytes) for IEEE binary128 standard. 1K-bits would result in 10 sections. L=32K bits would be divided into 320 sections instead of 352 sections. The summation would be less than 128 bits. The summation and the percentage distribution total data length approximates to 128 + 320 × 128 bits ≈ 40K vs. 44K as for Method1. The cost would be roughly (40-32)/32=12/32 = 25% traffic increase vs. 37.5%.

ICC with collective precision is made achievable with bipolar fuzzy sets defined in the quantum lattices or Cartesian products including $B_1 = \{-1,0\}\times\{0,+1\}$, $B_F = [-1,0]\times[0,+1]$, and $B_\infty = [-1,0]\times[0,+1]$, respectively, as shown by **Fig. 1**.

Bipolar fuzzy sets forms an equilibrium-based mathematical abstraction—a set theoretic or information theoretic generalization of classical sets and fuzzy sets. Bipolar fuzzy sets are quantum sets that provide a basis for logically definable causality and quantum intelligence *[15]*. Within the generalization, truth-based computing can be used freely as long as equilibrium conditions are not violated.

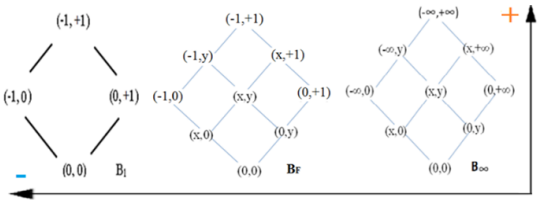


Figure 1. Hasse diagrams of YinYang bipolar quantum-fuzzy lattices B_1, B_F, B_∞ (adapted from *[12,13,14]*)

In this subsection, we show an ICC example with collective precision. A key concept is an information conservational bipolar matrix *M*. With a percentage distribution built into *M*, an energy or information total or summation can be decrypted through equilibrium-based rebalancing to result in all the subtotals in parallel. This makes it possible to develop digital or quantum machinery with massive parallelism and collective precision that is not achievable with a linearly normalized percentage distribution.

M consists of bipolar elements. A bipolar element is an energy/information import-export or negative-positive variable $x = (a^-, b^+)$ defined as the length of the bipolar interval from a to b. The energy/information of x is defined as $\varepsilon|x|$ as in *Eq. 2*. For instance, $|\varepsilon|(-2.5, 3.5)| = 3.5-2.5 = 2.5+3.5 = 6$.

$$\varepsilon|x| = \varepsilon|(a^-, b^+)| = b^+ - a^- = |a^-| + |b^+|. \qquad (2)$$

A 3-partner US-China-EU trade example is used to illustrate the basic idea of ICC with collective precision. First, the 3-parners' bipolar import-export data for 2014 are shown in **Fig. 2a** as a cognitive map (CM) in million Euros. The total energy/information in the trade scenario is characterized by the total import-export
$|\varepsilon|(-3030750, +0)| = \varepsilon|(-0, +3030750)| = 3030750$.

Using collective bipolar interaction in ICC, accurate calculation can be carried out with the bipolar quantum cellular automaton (BQCA) $E(t+1) = M \times E(t)$ based on a column-major normalized bipolar matrix *M* that does not need sequential calculation of a percentage distribution. (Note: The illustrations in this paper are in fixed-point format for readability. In real computing, they are in floating-point format.)

In this ICC example *E(1)* is the transpose of the initial bipolar column vector with certain total energy/information. A cognitive map (CM) *C* is referred to as a bipolar or unipo-

lar conceptual graph or an import/export network. *M* is obtained with column-major normalization of an I/O-consistent and interactive CM in which all elements are directly or indirectly interrelated *[6,7]*. We have

$$C(t) = \begin{bmatrix} (0,0) & (-420{,}079, +111{,}308) & (-311{,}035, +206{,}127) \\ (-111{,}308, +420{,}079) & (0,0) & (-164{,}777, +302{,}049) \\ (-206{,}127, +311{,}035) & (-302{,}049, +164{,}777) & (0,0) \end{bmatrix};$$

$$M = normalize(C^T(t)) = \begin{bmatrix} (0.000\ 0.000) & (-0.112\ 0.421) & (-0.209\ 0.316) \\ (-0.401\ 0.106) & (0.000\ 0.000) & (-0.307\ 0.167) \\ (-0.297\ 0.197) & (-0.165\ 0.303) & (0.000\ 0.000) \end{bmatrix}$$

Equilibrium-based rebalancing is illustrated in **Fig. 2b** and curved in **Fig. 2c**. **Fig. 2d** verifies such rebalancing with sequential computing. **Fig. 2e** shows 200% is rebalanced to a perfect percentage distribution built in *M*. Thus, matrix *M* can be deemed a quantum encryption of a percentage distribution. Here both of a quantum world and a classical world are logically unified in to a formal analytical paradigm without using bra-ket notation.

Equilibrium-based rebalancing can balance a total or a set of subtotals to a perfect equilibrium state with percentage distribution coded in *M* in an iterative and massively parallel process. Although a perfect equilibrium-state may be neither practical nor desirable in economics, equilibrium-based rebalancing provides a new approach to pre- and post-quantum cryptography. It finds a mathematical abstraction for collective precision and bridges the classical and quantum worlds.

S-OTP-Method2

Assume IEEE binary128 is used with the precision of 112 significant bits, and assume sender Alice and receiver Bob share private key K_1 distributed through QKD.

Part I. Encryption

Step 1. Data Transformation. *Given binary data D to be transmitted, let the unsigned integer number set $\{x_i\} = \{x_1, x_2, .., x_i, .., x_n\}$ represent preprocessed data sections of D and let math summation $X = \sum_i x_i$, $1 \le i \le N$,.*

Step 2. Bipolar Cognitive Mapping. *Construct an I/O-consistent bipolar cognitive map C based on $\{x_i\}$ such that $\{x_i\}$ is decomposed into an unbalanced relational data set $\{e_{ij}\} = \{(e_{ij}^-, e_{ij}^+)\}$ where each bipolar link weight $e_{ij} = (e_{ij}^-, e_{ij}^+)$ and $|d_i| \equiv \sum_j |\varepsilon| e_{ij}$ (energy/information of row i) with ratio $|e_{ij}^-|/|e_{ij}^+| > l$, a threshold for non-zero bipolar elements. Thus, the set $\{e_{ij}\}$ forms a bipolar cognitive map C with total information $X = \sum_i |x_i|$. (Note: C is not unique – an area of further research where bipolar linguistic fuzzy sets can be used for the optimization.)*

Step 3. Bipolar Energy/Information Normalization. *Normalize transpose C^T to an information conservational matrix M (a bipolar quantum-fuzzy logic gate (BQFLG) or a bipolar quantum-fuzzy cognitive map (BQFCM)) following Eq. 4 such that the BQCA $E(t+1) = M \times E(t)$ is asymptotic to an equilibrium state [6,7].*

Step 4. Data Encryption. *Use K_1 to encipher X and part of M to X', and apply Eq. 1 to change the remaining terms of M to a misleading M'';*

Step 5. Transmit the pair E = *(X',M'').*

Part II. Decryption

Step 1. *Use K_1 and Eq. 1 to recover the pair (X,M);*

Step 2. *Use M to decipher and depolarize X to recover $\{x_i\}$;*

Step 3. *Recover D from $\{x_i\}$ with concatenation.*

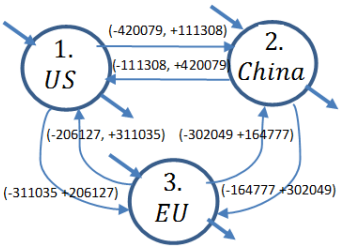
Illustration. Applying S-OTP-Method2 we have the decryption example in **Fig. 2**. The total information of the last row of **Fig. 2b** approximate to exactly the same result as that of S-OTP-Mehrod1:

$d_1 = |\varepsilon|(-731114, +317435) = 1048549$;

$d_2 = |\varepsilon|(-276085, +722128) = 998213$;

$d_3 = |\varepsilon|(-508176, +475812) = 983988$

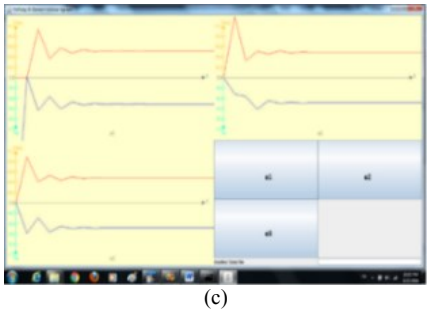
$D = Concatenate(d_1, d_2, d_3) = 1048549998213983988$.



(a)

t	E(t+1) = M(t) × E(t) e1	e2	e3
1	(-3030750.000, 0.000)	(-0.000, 0.000)	(-0.000, 0.000)
2	(0.000, 0.000)	(-321727.188, 1214205.875)	(-595794.188, 899022.625)
3	(-647442.250, 955835.875)	(-375738.375, 333436.250)	(-297782.688, 420514.375)
4	(-377520.813, 377520.813)	(-630613.250, 522677.375)	(-579544.938, 542872.625)
5	(-620577.625, 583280.625)	(-455013.250, 460129.250)	(-463296.094, 448453.000)
6	(-483180.125, 483180.125)	(-514797.813, 527851.500)	(-508652.563, 513087.688)
7	(-543767.625, 548278.250)	(-487545.188, 486926.438)	(-481218.563, 483013.688)
8	(-512763.688, 512763.688)	(-506231.313, 504652.594)	(-497437.406, 496901.063)
9	(-530639.875, 530094.375)	(-495690.813, 495765.688)	(-489388.063, 489170.938)
10	(-521049.438, 521049.469)	(-500810.844, 501001.781)	(-493386.656, 493451.531)
11	(-525948.625, 526014.563)	(-498152.719, 498143.656)	(-491231.906, 491258.156)
12	(-523370.719, 523370.719)	(-499627.813, 499604.750)	(-492391.719, 492383.844)
13	(-524756.813, 524748.875)	(-498834.719, 498835.813)	(-491788.219, 491785.063)
14	(-524021.125, 524021.125)	(-499249.156, 499251.906)	(-492102.594, 492103.531)
..	..	..	..
29	(-524274.313, 524274.313)	(-499106.281, 499106.281)	(-491993.781, 491993.781)
30	(-524274.250, 524274.250)	(-499106.281, 499106.281)	(-491993.781, 491993.781)
31	(-524274.250, 524274.250)	(-499106.250, 499106.250)	(-491993.750, 491993.750)
32	(-524274.250, 524274.250)	(-499106.250, 499106.250)	(-491993.750, 491993.750)

(b)



(c)

Partner	Import-Export of 2014	Total Volumes	Percentage (%)
US	(-731114 +317435)	1048549	1048549/3030750 = 34.5970%
China	(-276085 +722128)	998213	998213/3030750 = 32.9362%
EU	(-508176 +475812)	983988	983988/3030750 = 32.4668%
Total	(-1515375 +1515375)	3030750	100.0000%

(d)

t	E(t+1) = M(t) × E(t) Rebalancing 100 Percentage to Actual Distribution US	China	EU
1	(-100.0000, 100.0000)	(-0.0000, 0.0000)	(-0.0000, 0.0000)
2	(0.0000, 0.0000)	(-50.6783, 50.6783)	(-49.3217, 49.3217)
3	(-52.9004, 52.9004)	(-23.3993, 23.3993)	(-23.7003, 23.7003)
4	(-24.9127, 24.9127)	(-38.0530, 38.0530)	(-37.0343, 37.0343)
5	(-39.7215, 39.7215)	(-30.1952, 30.1952)	(-30.0833, 30.0833)
6	(-31.8852, 31.8852)	(-34.4024, 34.4024)	(-33.7125, 33.7125)
7	(-36.0322, 36.0322)	(-32.1528, 32.1528)	(-31.8150, 31.8150)
..	..	..	..
22	(-34.5969, 34.5969)	(-32.9362, 32.9362)	(-32.4669, 32.4669)
23	(-34.5971, 34.5971)	(-32.9361, 32.9361)	(-32.4668, 32.4668)
24	(-34.5970, 34.5970)	(-32.9362, 32.9362)	(-32.4668, 32.4668)
25	(-34.5970, 34.5970)	(-32.9362, 32.9362)	(-32.4668, 32.4668)

(e)

Figure 2. (a) Bipolar CM of 2014 US-China-EU trade (in Million Euros); (b) Rebalancing of total import/export to an equilibrium state; (c) Curves of the rebalancing; (d) Digital computing; (e) Quantum-fuzzy rebalancing of 200%

Theorem 6. S-OTP-Method2 is information conservationally secure provided that the summation is enciphered with a same length or longer S-OTP key and matrix *M* is made completely misleading and uncorrectable by an attacker without the key.

Proof. *It follows the proof for S-OTP-Method1.*

Remarks: (a) Theorem 6 closes a loophole in Theorem 8 of Ref. [6]. (b) The value of S-OTP-Method2 lies in its collective precision, not in key compression and data traffic. ■

3.3 The Quantum Intelligence Nature of ICC

The bipolar approach is based on a formal logic named bipolar dynamic logic and an algebra named bipolar quantum linear algebra, which are proven equilibrium-based bipolar dynamic generalizations of Boolean logic and linear algebra respectively. This development leads to an analytical quantum intelligence paradigm of ICC *[6,7]*.

Given an $n\times n$ square bipolar interactive matrix M and an $n\times 1$ column bipolar vector $E(t)$ such that $E(t+1)=M \times E(t)$, if the absolute energy/information subtotal $|\varepsilon_{col}|M_{*j}(t)$ of each column j of M equals 1.0 or, $\forall j$, $|\varepsilon_{col}|M_{*j}(t)\equiv 1.0$, M is referred to as an information conservational bipolar quantum logic gate (BQLG) matrix or a bipolar quantum-fuzzy cognitive map (BQFCM) *[6]*. With the BQLG matrix M we have a bipolar quantum cellular automaton (BQCA) (Eq. 3).

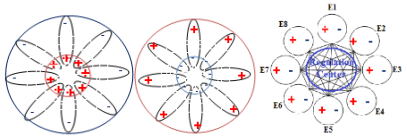
$$|\varepsilon|E(t+1) = |\varepsilon|(M \times E(t)) \equiv |\varepsilon|E(t). \quad (3)$$

Eq. 3 makes BQCA a general-purpose quantum cellular automata theory—an equilibrium-based unification of matter and antimatter atoms. Computationally, a BQCA can be regulated to achieve information conservation, regeneration, degeneration, and/or oscillation. It provides a basis for equilibrium-based quantum intelligence (QI) (**Fig. 3**) [6,7].

QI leads to the theory of ICC and S-OTP-Method2 with collective precision. In ICC, an I/O-consistent CM can always be designed and normalized to a BQLG matrix M for a BQCA to be asymptotic to a bipolar equilibrium state even though some link weights are weaker and need more iterations (t) to be balanced. This property provides a basis for pre- and post-quantum cryptography.

The transpose $C^T(t)$ is used to obtain its column-major normalized BQLG matrix M for ICC. The normalization follows Eq. 4. In Eq. 4, the denominator $|\varepsilon_{col}|(C^T_{*j})$ denotes the absolute energy/information subtotal of column j in C^T. The notation $|\varepsilon_{col}|(M_{*j})$ denotes the normalized absolute energy/information subtotal of column j of matrix M.

$$M(i,j) = (C^T(i,j))/|\varepsilon_{col}|(C^T_{*j}). \quad (4)$$



(a) (b) (c)

Figure 3. BQCA unification of matter and antimatter atoms (Adapted from *[16,17]*): (a) Matter; (b) Antimatter; (c) Unification

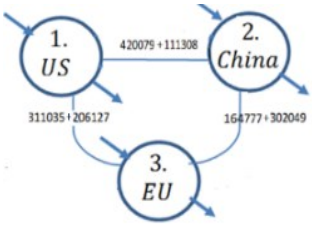
3.4 The Digital Nature of S-OTP-Method2

Notably, S-OTP-Method2 is based on bipolar equilibrium-based rebalancing**.** Bipolarity is a quantum feature that form the bipolar reality of negative-positive particles. The bipolar property, however, can be depolarized for digital cryptography. Thus, a unipolar CM can be revealed from a bipolar one with depolarization.

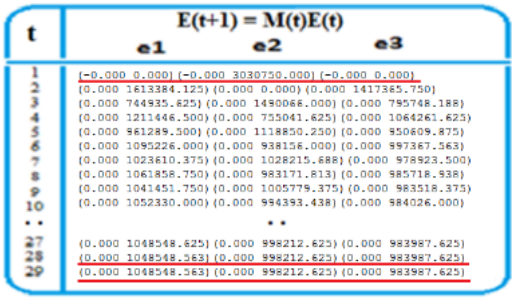
Since a bipolar representation is a generalization of unipolar representation and subsumes unipolar cases, all the elements of a polarized map can simply have zero negative energy/information which leads to the simplified CM as in **Fig. 4** coded as a unipolar matrix $C(t)$—a positive relation that does not distinguish import-export bipolarity.

Depolarization leads to a unipolar cipher that is basically the same as S-OTP-Method2 except using a positive *CM* and a positive matrix *M*. **Fig. 4** shows such a decryption example where in the last row we have the same result as for the bipolar case.

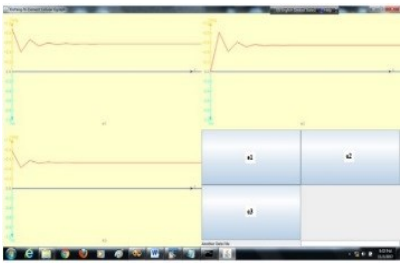
$d_1 = |\varepsilon|(-0, +1048549) = 1048549$;
$d_2 = |\varepsilon|(-0, +998213) = 998213$;
$d_3 = |\varepsilon|(-0, +983988) = 983988$;
$D = Concatenate(d_1, d_2, d_3) = 1048549998213983988$.



(a)



(b)



(c)

Figure 4. Information-conservational unipolar rebalancing: (a) depolarized CM; (b) Positive distribution; (c) Positive curve (scaled)

3.5 Two Puzzles Explained

(A) How can matrix C(t) in symmetry (C(t)(i,j)= C(t)(j,i)) be used in cryptography?

The answer is that, although matrix *C(t)* is symmetrical, a column-major normalized *M* can be non-linear and asymmetrical because the normalization is by dividing its column subtotal of $C^T(t)$, but not by the global total (corresponding to the overall summation). For instance,

$$C(t) = \begin{bmatrix} 0 & 531587 & 517162 \\ 531587 & 0 & 466826 \\ 517162 & 466826 & 0 \end{bmatrix};$$

$$M = \begin{matrix} 0 \\ 1 \\ 2 \end{matrix} \begin{bmatrix} 0.000 & 0.532 & 0.526 \\ 0.507 & 0.000 & 0.474 \\ 0.493 & 0.468 & 0.000 \end{bmatrix};$$

where *C* is symmetrical but *M* is not. The non-linear asymmetrical property of *M* can be characterized with a set of linear equations. Let the three subtotals (or data sections) be *x*, *y*, and *z*, respectively, for the 3×3 matrix *M* we have $m_{10}\times x - m_{01}\times y = 0$; $m_{20}\times x - m_{02}\times z = 0$; and $m_{21}\times y - m_{12}\times z = 0$; and $m_{ij} \neq m_{ji}$. The set of equations have infinite number of solutions because all column coefficients of *M* correlate non-linearly with each other due to non-linear normalization with different local column subtotals. This is fundamentally different

from percentage distribution where all percentages are normalized with a global total and linearly correlated.

(B) If a unipolar positive matrix is sufficient, why do we need a bipolar equilibrium-based matrix in cryptography?

There are four top answers to this question:

(i) The universe consists of negative-positive particles. Without bipolarity, there would be no information conservation, quantum intelligence, and bipolar quantum computing *[6,7]*. Thus, bipolarity leads to an analytical ICC paradigm compatible to digital computing (further discussed later).

(ii) Bipolarity is set-theoretically different from bilinearity or bijection, one defines a 2-to-2 mapping of equilibrium-based non-linear bipolar dynamic entanglement with logically definable causality and information conservation, another defines a 1-to-1 mapping without entanglement and definable causality. Of course, the negative sign can be eliminated with depolarization, but the bipolar semantics remains intact. **Fig. 5** shows the necessity of quantum bipolarity.

(iii) On the sender side, a bipolar matrix doubles the number of elements in a unipolar matrix, doubles the parallelism, avoids large denominators, and doubles collective precision with equilibrium-based rebalancing. On the receiver side, a bipolar matrix avoids decrypting a large total because, given a big integer E in 100%, we have the *equivalence law of energy/information distribution/conservation*:

$$|\varepsilon|E = |\varepsilon|\,[(-0, +100\%)] = |\varepsilon|[(-50\%, +50\%)]$$
$$= |\varepsilon|[(-25\%, +25\%))\ (-25\%, +25\%)] = |\varepsilon|[\ldots]. \qquad (5)$$

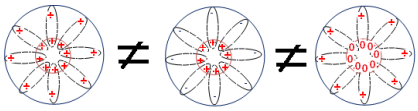


Figure 5. Necessity for quantum bipolarity

3.6 Minimal BQCA

Theorem 7 (Minimal BQCA Theorem). Summation and percentage distribution is a one-step bipolar quantum cellular automaton with all zero values for the negative poles. Thus, Mehtod1 would be the minimal case of Method2 if it could be optimized with collective precision.

Proof. *Mehtod2 entails an N×N square matrix multiplied by a column vector in an information conservational BQCA. When N×N is reduced to N×1, the matrix becomes a column vector of percentage distributions* $\{w_i\} = \{x_i/X\}$ *summing up to 1.0, the single number must be the summation X of N sections, such that the column vector multiplied by a single element matrix results in a column vector energy/information distribution* $\{x_i\}$*. The Matrix multiplication can be deemed the minimal BQCA which requires a final equilibrium state be reached in a single step such as* $\begin{pmatrix} w_0 \\ w_1 \\ w_{i+1} \\ w_n \end{pmatrix}[X] = \begin{pmatrix} x_0 \\ x_1 \\ x_{i+1} \\ x_n \end{pmatrix}$*. Thus, Mehtod1 would be the minimal case of Method2 if it could be optimized to have a minimum number of percentages with collective precision.* ■

The above theorem provides a unifying bridge between two mathematical abstractions, one for a bipolar quantum world and another for a classical unipolar world. Since Method1 is suitable for reducing network traffic and Method2 for optimization and collective precision, the two can now be combined in an optimization.

3.7 Optimization

Method1 uses percentage distribution; Method2 uses collective precision with a minimum number of percentages. In Method1 each data section depends on a single percentage resulted from linear normalization by a grand total. When the data length is long, Method1 will have a precision problem. In Method2, each data section depends on column-major

normalization by much smaller subtotals where percentage distribution is not directly calculated using a grant total as the denominator. If each column has an average of $n > 2$ nonzero numbers, the precision requirement is n-times smaller. The larger the number n the more parallelism in high precision decryption. When n equals N, Method2 reaches maximum parallelism with N-fold precision enforcement for a positive matrix M and $2N$-fold for a bipolar matrix M. This observation leads to the inception of information conservational *collective precision*.

Observation 1: Asymptoticity. If M is information conservational, a BQCA $E(t+1) = M \times E(t)$ is asymptotic to an equilibrium state as determined by M per references *[6,7]*.

Observation 2: Information Conservation. If an original message D is converted to an energy/information total E through a BQCA transformation, the information conservational matrix M of the BQCA can serve as a key to decode the total information to the original message D on the receiver side per ref. *[6]*. However, to transmit matrix M will cost much more than to transmit a percentage distribution. Thus, Method1 is more efficient than Method2 for network traffic but only Method2 can enable collective precision, optimization, and efficient decryption.

Theorem 8. If M is information conservational, a BQCA $E(t+1) = M \times E(t)$ can be used to derive the minimum number of percentages in a distribution embedded in M.

Proof. *Given $|\varepsilon|E(t) = 100$ (%), the theorem follows from the asymptoticity law [6] directly (e.g. Fig. 2e).* ■

Theorem 9. A percentage distribution of N divisions can be converted to an $N \times N$ (unipolar or bipolar) information conservational matrix M with collective precision with enhanced parallelism in decryption where M is information conservational and BQCA $E(t+1) = M \times E(t)$ is asymptotic to an equilibrium state.

Proof. *Notice that M is normalized and information conservational but not unique. The theorem follows from* $\begin{pmatrix} w_0 \\ w_1 \\ w_{i+1} \\ w_n \end{pmatrix}[E] = \begin{pmatrix} w_0E \\ w_1E \\ w_{(i+1)}E \\ w_nE \end{pmatrix}$ *because* $\begin{pmatrix} w_0 \\ w_1 \\ w_{i+1} \\ w_n \end{pmatrix}$ *is strictly proportional to* $\begin{pmatrix} w_0E \\ w_1E \\ w_{i+1}E \\ w_nE \end{pmatrix}$*. That is, M can be derived from either of the two column vectors.* ■

Based on the above findings we can conclude that, on the sender side, matrix M can be used for determining the minimum percentage distribution with collective precision that can achieve *N to 2N fold* reduction of precision requirement due to column-major normalization (Re. Eq. 4). On the receiver side, M can be used to decrypt a big total to subtotals (or data sections) with collective precision in a reverse way (**Fig. 2b** and **Fig. 4b**). Thus, Method1 and Method2 can be used in a combination. Method2 focuses on ICC with collective precision; Method1 focuses on secure and efficient data transmission, this lead to the block diagram design in **Fig. 6** that combines the advantages of Method1 and Method2 while eliminating drawbacks of each of them.

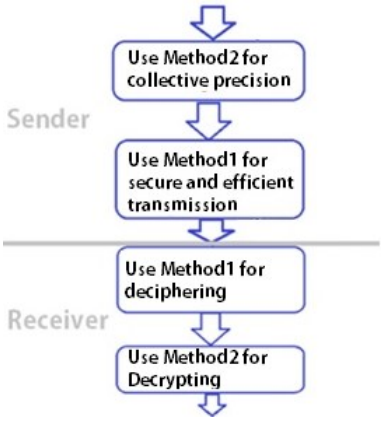


Figure 6. Method1 and Method2 combined

The combination of two methods together leads to an optimized algorithm named S-OTP-Method$_{1+2}$.

S-OTP-Method1+2

For 32K-bit binary data (more or less) divided into 320 (more or fewer) sections $\{x_i\}$, assume sender Alice and receiver Bob share private key K_1 distributed through QKD. An integer P is private until the sender found the number of concealed percentages. Assume no zero-value data section. Assume IEEE binary128 standard with 112 significant bits precision

Part I –Sender Side

Step 1. *Let integer set $\{x_i\}$ represent preprocessed data sections;*

Step 2. *Let math summation $X = \sum_i x_i$ for all i*

Step 3. *Use the collective precision advantage of Method2 to calculate percentage distribution $\{x_i/X\}$ (See Fig. 2e);*

Step 4. *Use Method$_1$ and K_1 to encrypt X and P terms of $\{x_i/X\}$ to X' and use Eq. 1 to encrypt the remaining (N - P) terms of the percentage distribution to $\{x_i/X\}$";*

Step 5. *Alice Transmits the pair E=(X', $\{x_i/X\}$") to Bob use Method$_1$.*

Part II. Receiver Side

Step 1. *Use K_1 and Eq. 1 to decipher E to recover the pair (X, $\{x_i/X\}$);*

Step 2. *Use $\{x_i/X\}$ to derive an information conservational matrix M so that Method$_2$ can be used to decrypt the summation X to $\{x_i\}$;*

Step 3. *Recover the message from $\{x_i\}$ with concatenation.*

Example. Assuming the plaintext data *D* to be transmitted is represented by the big integer *L = 1048549998213983988* divided into the three sections *1048549, 998213, and 983988.* Assume sender Alice and receiver Bob share K_1 distributed through QKD.

Part I – Encryption (some steps are omitted)

- *Let x_1 =1048549, x_2 = 998213, x_3 = 983988;*
- *X = $x_1 + x_2 + x_3$= 3030750;*
- *Use Method2 to calculate percentage distribution (see **Fig. 2(e)**) and $\{x_i/X\}$ = {34.5970%, 32.9362%, 32.4668%};*
- *Use Method1 to encrypt (X, $\{x_i/X\}$) to (X, $\{x_i/X\}$)' and transmit;*

Part II – Decryption (some steps are omitted):

- *Use K_1 and Eq. 1 to decrypt the message;*
- *U=(3030750, {34.5970%, 32.9362%, 32.4668%});*
- *Derive an information conservational BQCA based on U using Method2;*
- *Use the BQCA and Method2 to decrypt U (see Method2 and **Fig. 2(b)**);*
- *x_1 = 1048549, x_2 = 998213, and x_3 = 983988;*
- *L = concatenate(x_1, x_2, x_3) = 1048549998213983988;*
- *Recover D from L.*

It should be noted that the above example illustrates the basic concept but may be too small to be fully illustrative to the collective precision property of Method2. With a large number of sections, collective precision would be crucial. In that case, Method1 would face a precision problem due to a huge summation denominator. Method2, however, does not have to deal with the big summation. Thus, collective precision could spark an analytical paradigm of ICC supercomputing machinery with analytical quantum intelligence.

Theorem 10. S-OTP-Method1+2 is information conservationally secure provided that S-OTP-Method1 is secure.

Proof. *Since Method2 is only used for optimization with collective precision but not for communication, the theorem follows the proof for S-OTP-Method1 directly.* ■

3.8 Hierarchical Extension

S-OTP-Method1+2 can be extended to a hierarchical algorithm with BHKC/BBDR. With BHKC, a hierarchical process of ICTs can scale down or reduce an OTP keypad length for a long message to a condensed tiny minimum. Taking QKD cost saving into consideration the benefit of BHKC/BBDR significantly overweighs the cost.

S-OTP-Hierarchical

Assume IEEE binary128 is used with the precision of 112 significant bits, and assume the sender and receiver share private key K_1. Assume preprocessed data sections.

Part I –Sender Side BHKC

Step 1. Level L = 0; OTP key length required equals to data length, that is not practical for long messages of multiple mega or gaga bits; let block index b = 0; let total number of blocks B = (total number of bits)/32K;

Step 2. Level L = L+1, for each 32K-bit (longer or shorter) data block, apply S-OTP-Method$_{1+2}$ to reduce the key length to 2K, 4K, or 8K compressed data bits, respectively, as designated, to conceal a 128-bit summation and P terms of percentages. Total key length is reduced after this step by 32-, 16-, or 8-folds, respectively, as designated. The unconcealed percentages are made completely misleading and uncorrectable by an attacker without private key. The compressed data for each 32K are left for further compression without enciphering;

Step 3. If total key length for compressed data is greater than 2K, 4K, or 8K bits as designated, go to Step 2;

Step 4. Encipher the compressed data with K_1 and encrypt the remaining percentages with Eq. 1.

Step 5.Transmit the ciphertext and all the misleading percentages for each 32K-bit data block at each level to the receiver.

Part II – Receiver Side BBDR

Step 1. *Use S-OTP-Method$_{1+2}$ to decipher with K_1;*

Step 2. *L = L – 1; if L > 0, go to Step (1);*

Step 3. *Recover the original message or data set D by concatenating the data sections.*

Figures 7a and 7b show the sketches of BHKC and BBDR, respectively.

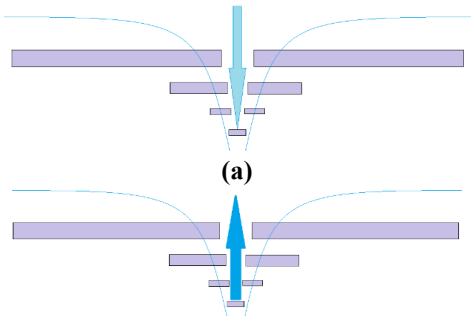


Figure 7. Sketches: (a) BHKC; (b) BBDR

BHKC Example 1. Given a 64G-bit long message (or shorter), assuming 32-fold key reduction for each round of ICT,

- *L = 0, total key length = 64G bits, impractical and not applicable;*
- *L = 1, total key length = 64G/32 = 2G, impractical and not applicable;*
- *L = 2, total key length = 2G/32 = $2^{11}M/2^5 = 2^6M$ = 64M, impractical and not applicable;*
- *L = 3, total key length = 64M/32 = 2M, impractical and not applicable;*
- *L = 4, total key length = 2M/32 = $2^{11}K/2^5 = 2^6K$ = 64K, impractical and not applicable;*
- *L = 5, total key length = 64K/32 = 2K, practical key applied.*

BHKC Example 2. For the same problem as in Example 1 but assuming 16-fold key reduction for each round of ICT instead of 32-fold, we have

- *L = 0, total key length = 64G bits, impractical and not applicable;*
- *L = 1, total key length = 64G/16 = 4G, impractical and not applicable;*
- *L = 2, total key length = 4G/16 = $2^{12}M/2^4 = 2^8M$ = 256M, impractical and not applicable;*
- *L = 3, total key length = 256M/16 = 16M, impractical and not applicable;*
- *L = 4, total key length = 16M/16 = 1M = $2^{10}K$, impractical and not applicable;*
- *L = 5, total key length = $2^{10}K$ /16 = 64K, impractical and not applicable;*

- *L = 6, total key length = 64K/16 = 4K, practical and applied.*

Theorem 11. S-OTP-Hierarchical is information conservationally secure provided that S-OTP-Method1+2 is secure.

Proof. *Since the section percentages in different data blocks at different layers are not correlated in anyway, the theorem follows Theorems 10 and 11 directly.* ■

With S-OTP-Hierarchical, sender-receiver collusion on collective precision could be important. On the sender side, collective precision can be used for testing intermediate results efficiently and precisely to guarantee that the receiver side will get the correct message. On the receiver side, it can be used to decrypt the total to many subtotals precisely and efficiently in massive parallelism. The two sides can be colluded through public protocols based on the ranges of data length and number of sections.

Clarification 4. As we know information (message) is ultimately presented as binary (0/1) bits in modern computing and communication, this leads to the question:

When we scale an OTP keypad to a tiny S-OTP key through BHKC, is there really no information (entropy) loss during the process?

The answer to the above question is that there is neither information loss nor information leaking. Since ICS/S-OTP does not reduce data length with a limited network traffic increase as a tradeoff, "black hole" keypad compression does not cause information loss within the limit of computational precision. In addition, since collective precision can be colluded based on certain public protocol between a sender and a receiver, "big bang" data recovery is guaranteed full data recovery.

It should be pointed out, however, that a tiny keypad for transmitting a long message without information loss does not suggest unsecure information leaking in anyway. S-OTP transforms a long message into a large number of isolated, semantically meaningless, and holistically interlocked little pieces using percentage-based information conservational key extension (PBICKE) where an original message can only be holistically recovered with the condensed private S-OTP key equivalent to an OTP key. Otherwise, no deterministic algorithm can break it because ICS/S-OTP does not weaken ITS/OTP as axiomatically proven.

4. QUANTUM EXTENSION

While collective precision adds a number of new features to cryptography, its biggest potential could be its equilibrium-based extension of quantum mechanics and quantum computing to an equilibrium-based analytical paradigm. It further suggests that Method2 is suitable for developing bipolar quantum-digital compatible ICC machinery. While the illogical aspect of bra-ket quantum mechanics prevents quantum computing from becoming an analytical paradigm, ICC makes the quantum dream logically possible and quantum-digital compatible with a formal set-theoretic theory of quantum intelligence.

From a security perspective, quantum-digital compatible ICC machinery can be an ultimate solution to achieve perfect security. Although ITS/OTP is widely believed the only unbreakable crypto system even if the adversary has unlimited computing power, the optimality paradox as proven in Theorems 1-3 cast doubt on this claim from the perspective of ICS. Even though researchers are trying hard to find a solution for post-quantum cryptography, a perfect digital computing solution may not exist. If quantum-proof cryptography is not realizable through digital communication, the only option left for post-quantum cryptography could be quantum teleportation. Bipolar quantum entanglement provides such an equilibrium-based logical basis *[6,7]*.

The nature of S-OTP-Mehtod2 makes it suitable for equilibrium-based bipolar quantum rebalancing with perfect information conservation. Encryption would be unnecessary for quantum communication as any attack to a quantum channel would jeopardize perfect information conservation and stop the communication. Such a quantum teleportation machine is drafted in **Figs. 8(a,b,c)**. **Fig. 8(a)** sketches a bipolar quantum-digital compatible ICC crypto machine. **Fig. 8(b)** sketches bipolar quantum teleportation. **Fig. 8(c)** portrays a bipolar qubit register. **Fig. 8(d)** tables YinYang bipolar universal modus ponens (BUMP)

as an ubiquitous law for bipolar quantum entanglement with definable causality—a logical basis for bipolar quantum teleportation.

While the bipolar quantum dream may still seem to be "far-fetched" in terms of quantum-digital compatibility for ICC, a newly reported discovery of a class of subatomic particles (fermions) *[18]* injected new life into this line of research. The new discovery is a family of particles that are their own antiparticles. This family of particles strengthen the ontological basis of equilibrium-based bipolar quantum rebalancing and may make quantum computing more practical and powerful.

The equilibrium-based architecture in Fig. 8 forms the basis of analytical quantum intelligence machinery. The significance of this new paradigm is further supported by the realization of quantum teleportation between long distances *[19,20]* that gives hope for practical application of ICC with perfect quantum information conservation and security.

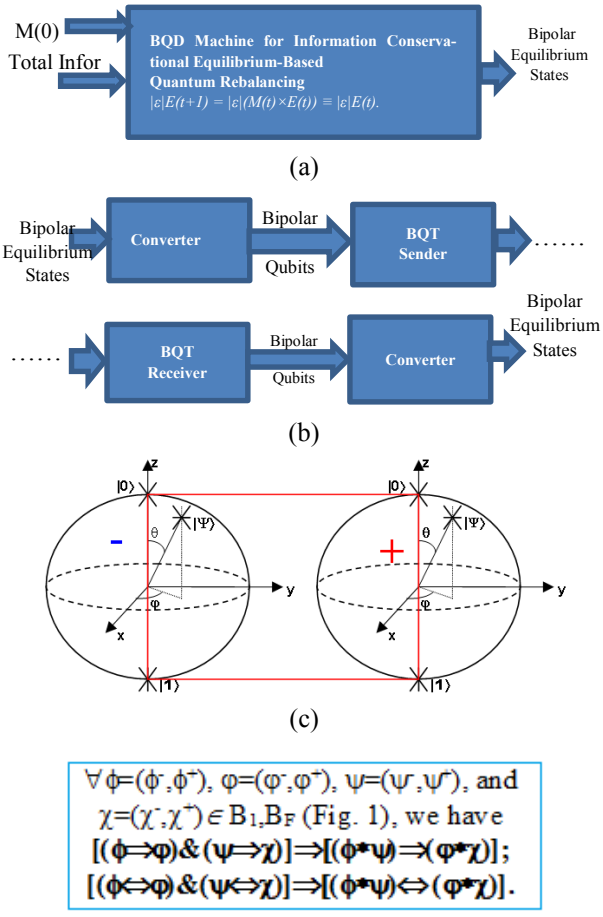


Figure 8. ICC—An Analytical Paradigm of Quantum Mechanics: (a) Bipolar quantum-digital compatible machinery; (b) Bipolar quantum teleportation (BQT); (c) Bipolar qubit register *[14,17];* (d) Bipolar universal modus ponens (BUMP)

5 CONCLUSIONS

Based on information conservational quantum intelligence *[6,7,15,21,22,23]*, information theoretic security has been extended to information conservational security that has led OTP to S-OTP. "Black hole" keypad compression coupled with "big bang" data recovery has been introduced for S-OTP with gains significantly overweigh costs. It is proven that if the security of OTP is optimal, S-OTP would be impossible; on the other hand, if S-OTP is not information theoretically secure, OTP would not be secure either. Thus, we

have a proof by contradiction on the paradoxical nature of OTP optimality from an information conservational perspective. The proof has further led to an analytical paradigm of quantum intelligence machinery toward perfect information conservational security. It has been shown that

- *S-OTP makes it possible for transmitting long messages or large data sets with a condensed tiny keypad for ICS that does not weaken ITS in its new context.*
- *Math summation with percentage distribution without using big primes makes S-OTP quantum proof to quantum factorization [1] for both pre- and post-quantum cryptography.*
- *ICC with collective precision can be massively parallel, accurate, efficient, and suitable for developing supercomputers with digital technology.*
- *ICC is quantum-digital compatible and suitable for developing teleportation machinery with perfect information conservation and quantum security.*
- *It has been shown that a summation with percentage distribution is a minimal/special case of equilibrium-based bipolar quantum cellular automata. This finding has made it possible to combine the advantages of both approaches for pre-and post-quantum cryptography, one for efficient and minimum data communication and another for effective and acurate computation with collective precision. On the other hand, the finding has unified a classical world with the quantum world in terms of mathematical abstraction.*

While bra-ket notation *[24]* is adopted as a standard for quantum mechanics and quantum computing in general, the standard limits quantum computing within Hilbert space—a complex spacetime geometry that stopped short of providing logically definable causality for the Copenhagen interpretation *[25]*. With formal logically definable causality *[6, 7, 14, 15, 21]*, the quantum intelligence approach extends Bohr's particle-wave complementarity principle to a bipolar interpretation. It has led to an equilibrium-based analytical arm for research in quantum mechanics and quantum computing including but not limited to quantum information science (e.g. *[26,27]*), quantum life (e.g. *[28, 29, 0]*), and quantum cryptography (e.g. *[1, 2, 18, 19, 20, 31, 32, 33]*).

Whereas OTP has been prevented from being widely used by its key length requirement, S-OTP has got around the problem through ICC without weakening ITS in its new context. Thus, S-OTP qualifies itself as a unique extension from information theoretic security to information conservational security. While this work has been focused on information conservational security, the equivalency or non-equivalency between ICS and ITS with different entropy measures (ex. *[34]*) may deserve further investigation.

Floor-Roof Mysteries. According to the floor-roof theory of science *[15,23],* ITS of OTP has been developed based on information theory rooted in probability and statistics—a floor or foundation of modern science focused on observability and entropy without logically definable causality and bipolar information conservation. ICS of S-OTP, on the other hand, has been a set-theoretic development rooted in bipolar quantum intelligence—a roof of modern science focused on equilibrium-based rebalancing and information conservation with logically definable causality *[6,7]*. Thus, this work has opened some major challenges to computing, cryptography, and science in general. Among them are the following floor-roof mysteries:

- *Is ICS an information theoretic extension to ITS or just a new technological development?*
- *Is ICS a falsification of ITS in terms of optimality?*
- *Is S-OTP just OTP plus data compression and there is nothing new?*
- *Shannon concluded on the impossibility for perfect secrecy beyond OTP with key length greater than or equal to the message to be enciphered [3]. Although this paper did not attempt to falsify the theorem directly, however, if S-OTP is secure, could Shannon's theorem be wrong? On the other hand, if ICS of S-OTP is not secure, could ITS of OTP be secure?*
- *Could modern science, such as modern physics and information theory [3,4], have been like a well-founded building with a floor of observable beings and truths but missing its roof for equilibrium, harmony, information conservation, and logically definable causality [6, 7, 5, 21, 2, 23]?*

Floor-Roof Assertions. Despite the mysteries, we have the following floor-roof assertions:

- *Can the floor perform some functions not performed by the roof? The answer is definitely YES.*
- *Can the roof perform some functions not performed by the floor? The answer is definitely YES.*
- *Can information conservational security solve some unsolved problems by information theoretic security? The answer should be LOGICALY YES.*
- *Does modern science need information conservation and logically definable causality as its roof? The answer should be LOGICALY YES.*

ACKNOWLEDGEMENT

The author acknowledges his colleague Professor Kai Wang in Computer Science Department of Georgia Southern University for his input in double precision floating-point computing. The author acknowledges the anonymous reviewers for their valuable review comments. Two earlier versions of this work were submitted to and considered by *Science* and *Nature*, respectively.

REFERENCE

[1] P. Shor (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proc. 35th Annual Symposium on Foundations of Computer Science*, 1994, 124-134.

[2] Daniel J. Bernstein & Tanja Lange (2017). Post-quantum cryptography. *Nature,* volume 549, pp188–194 (14 Sept. 2017)

[3] C. Shannon (1949). Communication Theory of Secrecy Systems. *Bell System Technical Journal* **28** (4): 656–715.

[4] C. Shannon (1948). A Mathematical Theory of Communication. *Bell System Technical Journal. **27** (3):379–423.*

[5] W.-R. Zhang (2018). Scalable One-Time Pad—From Information Theoretic Security to Information Conservational Security. Unpublished Tech. Report. https://eprint.iacr.org/2018/1095.pdf.

[6] W.-R Zhang (2017). From Equilibrium-Based Business Intelligence to Information Conservational Quantum-Fuzzy Cryptography — A Cellular Transformation of Bipolar Fuzzy Sets to Quantum Intelligence Machinery. *IEEE Explore 3/24/2017*, *IEEE Trans. on Fuzzy Systems***,** Volume: 26, Issue: 2, April 2018, 656 – 669.

[7] W.-R. Zhang (2017). Programming the Mind and Decrypting the Universe — A Bipolar Quantum-Neuro-Fuzzy Associative Memory Model for Quantum Cognition and Quantum Intelligence. *Proc. of Int'l J. Conf. on Neural Networks (IJCNN 2017),* Anchorage, Alaska, USA, May 14–19, 2017, 1180 - 1187.

[8] Robert Morris, Ken Thompson (1978). *Password Security: A Case History*. Archiaved, Bell Laboratories.

[9] Sahai A, Waters B. (2004). Fuzzy identity-based encryption. In: Cramer R, editor. Advances in cryptology – EUROCRYPT 2005, vol. 3494. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 2005. p. 457–73.

[10] Y Zhang, X Chen, J Li, DS Wong, H Li, I You (2017). Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing. *Information Sciences* 379, 42-61

[11] J Li, Y Zhang, X Chen, Y Xiang (2018). Secure attribute-based data sharing for resource-limited users in cloud computing. Computers & Security 72, 1-12

[12] W.-R. Zhang (1998). YinYang Bipolar Fuzzy Sets. *Proc. of IEEE World Congress on Computational Intelligence*, Anchorage, Alaska, May, 1998, Fuzz-IEEE pp835-840.

[13] W.-R. Zhang and L. Zhang (2004), "YinYnag Bipolar Logic and Bipolar Fuzzy Logic." *Information Sciences*, Vol. 165, 3-4, 2004, pp265-287, (Elsevier).

[14] W.-R. Zhang (2011), *YinYang Bipolar Relativity: A Unifying Theory of Nature, Agents and Causality with Applications in Quantum Computing, Cognitive Informatics and Life Sciences*. IGI Global, Hershey and New York, 2011.

[15] W.-R. Zhang (2019), The Road from Fuzzy Sets to Definable Causality and Bipolar Quantum Intelligence — To The Memory of Lotfi A. Zadeh. *Journal of Intelligent & Fuzzy Systems*. vol. 36, no. 4, pp. 3019-3032, 2019, IOS Press.

[16] W.-R. Zhang (2012). YinYang Bipolar Atom – An Eastern Road toward Quantum Gravity. *J. of Modern Physics*, 2012, 3, 1261-1271. (open access) DOI: 10.4236/jmp.2012.329163.

[17] W.-R. Zhang (2013). Bipolar Quantum Logic Gates and Quantum Cellular Combinatorics — A Logical Extension to Quantum Entanglement, *J. of Quantum Information Science*, Vol. 3 No. 2, 2013, pp. 93-105. (open access) DOI: 10.4236/jqis.2013.32014.

[18] Q. L. He; Lei Pan; Alexander L. Stern; Edward C. Burks; Xiaoyu Che; Gen Yin; Jing Wang; Biao Lian; Quan Zhou; Eun Sang Choi; Koichi Murata; Xufeng Kou; Zhijie Chen; Tianxiao Nie; Qiming Shao; Yabin Fan; Shou-Cheng Zhang; Kai Liu; Jing Xia; Kang L. Wang (2017). Chiral Majorana fermion modes in a quantum anomalous Hall insulator–superconductor structure. *Science* 21 Jul 2017: Vol. 357, Issue 6348, pp. 294-299

[19] Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, Guang-Bing Li, Qi-Ming Lu, Yun-Hong Gong, Yu Xu, Shuang-Lin Li, Feng-Zhi Li, Ya-Yun Yin, Zi-Qing Jiang, Ming Li, Jian-Jun Jia, Ge Ren, Dong He, Yi-Lin Zhou, Xiao-Xiang Zhang, Na Wang, Xiang Chang, Zhen-Cai Zhu, Nai-Le Liu, Yu-Ao Chen, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, Jian-Wei Pan (2017). Satellite-based entanglement distribution over 1200 kilometers. *Science* 16 Jun 2017: Vol. 356, Issue 6343, pp. 1140-1144. DOI: 10.1126/science.aan3211

[20] Adam D. Cohen (2019). Advancement in Quantum Entanglement Earns 2018 AAAS Newcomb Cleveland Prize. *AAAS News Report*, 31 January 2019.

[21] W.-R. Zhang and K. E. Peace (2014). Causality Is Logically Definable — Toward an Equilibrium-Based Computing Paradigm of Quantum Agent and Quantum Intelligence (QAQI) (Survey and Research). *Journal of Quantum Information Science*, Vol. 4, 227-268. (open access) DOI: 10.4236/jqis.2014.44021.

[22] W.-R. Zhang (2016). G-CPT Symmetry of Quantum Emergence and Submergence – An Information Conservational Multiagent Cellular Automata Unification of CPT Symmetry and CP Violation for Equilibrium-Based Many World Causal Analysis of Quantum Coherence and Decoherence. *J. of Quantum Infor. Sci.*, Vol. 6, No. 2, 2016, pp. 62-97. (open access) DOI: 10.4236/jqis.2016.62008.

[23] W.-R. Zhang (2018). A Logical Path from Neural Ensemble Formation to Cognition with mind-light-matter unification—The Eternal Dow Can Be Told.. *Int'l J. of Cognitive Informatics and Natural Intelligence,* Vol. 12, No. 4, Oct-Dec. 2018, pp20-54.

[24] P. Dirac. (1930). *The Principle of Quantum Mechanics.* 4th Edition, Oxford University Press Inc., New York, Reprinted, 2004.

[25] N. Bohr (1948), On The Notions of Causality and Complementarity. *Dialectica*, Vol. 2, 3-4, 312–319, 1948.

[26] S. Lloyd (2007), *Programming the Universe — A Quantum Computer Scientist Takes on the Cosmos*. Alfred A. Knopf, Inc.

[27] W.-R. Zhang and Peace, K.E. (2013) Revealing the Ubiquitous Effects of Quantum Entanglement—Toward a Notion of God Logic. *Journal of Quantum Information Science*, **3**, 143-153. http://dx.doi.org/10.4236/jqis.2013.34019

[28] Derek Abbott, P C W Davies, and Arun K Pati (Editors) (2008). *Quantum aspects of life*. Imperial College Press, London. (Forward by Sir Roger Penrose)

[29] W.-R., Zhang, A. Pandurangi & K. Peace (2007). YinYang Dynamic Neurobiological Modeling and Diagnostic Analysis of Major Depressive and Bipolar Disorders. *IEEE Trans. on Biomedical Engineering,* Oct. 2007 54(10):1729-39.

[30] W.-R. Zhang, H. J. Zhang, Y. Shi & S. S. Chen (2009). Bipolar Linear Algebra and YinYang-N-Element Cellular Networks for Equilibrium-Based Biosystem Simulation and Regulation. *J. of Biological Systems*, Vol. 17, No. 4, 2009, 547-576. (WSP)

[31] Xiangfu Zou, Daowen Qiu (2013). Attack and improvements of fair quantum blind signature schemes , *Quantum Information Processing*, 2013, 12(6):2071-2085

[32] Xiangfu Zou, Daowen Qiu, Fang Yu, Paulo Mateus (2014). Security Problems in the Quantum Signature Scheme with a Weak Arbitrator, *International Journal of Theoretical Physics*, 2014,53(2): 603-611

[33] Wei Zhang, Daowen Qiu, Xiangfu Zou (2016). Improvement of a quantum broadcasting multiple blind signature scheme based on quantum teleportation, *Quantum Information Processing*, 2016, 15(6): 2499-2519

[34] Rényi, Alfréd (1961). On measures of information and entropy. *Proceedings of the fourth Berkeley Symposium on Mathematics, Statistics and Probability* 1960. pp. 547–561.