EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
Vol. 14, No. 2, 2021, 521-536
ISSN 1307-5543 – ejpam.com
Published by New York Business Global

Group and cipher in wormhole and quantum entanglement

Yonghong Liu

School of Automation, Wuhan University of Technology, 205 Luoshi Road, Wuhan, China

Abstract. In this article, we present wormholes cryptosystems (WCS). The first is the wormhole key distribution centre theorem, which asserts that the WCS is a public key group. The second is the security theorem, which asserts that the WCS are a one-way function. The third is new version of the definition for the WCS, and we introduce the notion of groups of WCS. The fourth ingredient is the encryption algorithm and decryption algorithm, and design principle. Here, we present a toy example to illustrate the computation of these encryptions and decryptions. The finally we present the unsymmetrical WCS theorem.

2020 Mathematics Subject Classifications: 94A60, 81R12, 81P40

Key Words and Phrases: Groups, Cryptography, One-way function, Zero-knowledge proof, Quantum entanglement, Wormhole

1. Introduction

Quantum information science is an area of study based on the idea that information science depends on quantum effects in physics. The wormhole is a subject of fascination for the scientific community. It is interesting to note that the quantum entanglement has that honor that has put it in wormhole. Van Raamsdonk's essay originally published in the General Relativity and Gravitation [1] has been concerned; this illustrates the wormhole compatibility with the quantum entanglement. Maldacena and Susskind [2], Cowen [3] and others considered the problem of a related conjecture, i.e., ER = EPR [4]; it is a conjecture in physics stating that entangled particles are connected by a wormhole (or known as Einstein-Rosen bridge) [3]; the conjecture was proposed by Maldacena and Susskind [2]. Testing the ER = EPR hypothesis to see if it is mathematically consistent with everything else that is known about entanglement and wormholes, because it involves the establishment of new scheme for cryptography. Besides, it has long been theorized that secure asymmetric cipher all use the number theory. But one thing that is certain, it seems to be very difficult to prove anything about the security of a system if the encryption is deterministic. Shor [5] stated in 1994 that the discrete logarithms problem and factoring

DOI: https://doi.org/10.29020/nybg.ejpam.v14i2.3972

Email address: hylinin@whut.edu.cn (Y. Liu)

problem by the quantum algorithm can be solved in polynomial time. The quantum computers should be able to defeat encryption that is unbreakable in practice today, with people in desperate need of practical and secure public-key cryptosystems. In this paper, the wormholes cryptosystems (WCS) is a new public-key cryptosystem and wormhole key distribution (WKD) would be at the very heart of it. The WCS and the well-known RSA [6] are very different theories. WCS is a new public-key cryptosystem and wormhole key distribution (WKD) would be at the very heart of it. Emphasis here is on a rigorous algebraic approach to the WCS. It is based on a new group of the product of two large primes (p, q) and is a multiplication function $h(x, y, z)$ of wormholes, which is a one-way function. The product of these primes is a number of between about 200 and 600 decimal digits, cannot be factored in a reasonable length of time. In other words, the WKD encryption algorithm, there are from 2^{200} to 2^{600} mappings. Therefore, the WCS as a public-key cryptosystem are computational security. We can now establish the fact that makes the key distribution centre (KDC) interesting because we can give the physical explanation on rapid particles, and the wormhole key distribution centre (WKDC) is considered sufficiently secure in most situations.

2. Preliminaries

Let Ω be an arbitrary nonempty set. We denote by Pas (Ω) the set of all bijections from Ω to itself. These bijections on Ω are also so-called pseudo-associations, and if Ω finite, this is, of course, the new term. The object Pas (Ω) is called the group [4] on Ω, and subgroup of Pas (Ω), denoted by Pas ($\langle\Omega\rangle$), which we are about to define.

Definition 1. [4] Let Ω be an arbitrary set and let G be a group. We say that G is a Pas (Ω) on Ω is any nonempty subset $P \subseteq$ Pas (Ω) with the following properties:
(PAG1) P is closed under a pseudo associative binary operation $\bullet$.
(PAG2) For each $x \in P$, $1 \bullet x = x = x \bullet 1$.
(PAG3) For each $x \in P$, there exists $x^{-1} \in P$ such that $x \bullet x^{-1} = 1 = x^{-1} \bullet x$.
(PAG4) For all x, y, $z \in P$, $(x \bullet y) \bullet z = x \bullet (z \bullet y)$.

Definition 2. [4] A mirror is called quasi-group G with an identity element 1 with an associative binary operation $\bullet$ defined on G such that there exists $1 \in G$ if it satisfies the axioms:
(QUG1) $1 \bullet x = x = x \bullet 1$ for all $x \in G$ and
(QUG2) $1 \bullet (x \bullet y) = (1 \bullet y) \bullet x = y \bullet x$ for all x, $y \in G$.

Definition 3. [7] A BCL^+ algebra is a triple $(X; \bullet, 1)$, where X is a nonempty set, $\bullet$ is a binary operation on X, and $1 \in X$ is an element such that the following three axioms hold for any x, y, $z \in X$.
(BCL^+1) $x \bullet x = 1$.
(BCL^+2) $x \bullet y = 1$ and $y \bullet x = 1$ imply $x = y$.
(BCL^+3) $((x \bullet y) \bullet z) \bullet ((x \bullet z) \bullet y) = (z \bullet y) \bullet x$.

Definition 4. [8] If $(f(x,\, y,\, z),\, g(x,\, y,\, z)) = 1$, then we say that $f(x,\, y,\, z)$ and $g(x,\, y,\, z)$ are coprime topological groups $(Y,\, \Im,\, \bullet)$ for all $x,\, y,\, z \in Y$. Let $h(x,\, y,\, z)$, $f(x,\, y,\, z)$ and $g(x,\, y,\, z)$ be ternary polynomial. Suppose the following conditions hold:
(WHT1) $h(x,\, y,\, z) = (z \bullet y) \bullet x$.
(WHT2) $f(x,\, y,\, z) = (x \bullet y) \bullet z$.
(WHT3) $g(x,\, y,\, z) = (x \bullet z) \bullet y$.

Definition 5. [7] If

$$(h(x,\ y,\ z),\ f(x,\ y,\ z)) = 1 \tag{1}$$

and

$$(h(x,\ y,\ z),\ g(x,\ y,\ z)) = 1, \tag{2}$$

then

$$(h(x,\ y,\ z),\ f(x,\ y,\ z)\ \bullet\ g(x,\ y,\ z)) = 1. \tag{3}$$

Theorem 1. [4] *Let G be a group with an associative multiplication and suppose there exist unique element $x,\, y \in G$ such that*

$$x\ \bullet\ y = 1\ \bullet\ (y\ \bullet\ x). \tag{4}$$

Then G is a commutative group or abelian.

We think of a public-key system in terms of an abstraction called a one-way function more precise, as follows.

Definition 6. A function f is a one-way function if
(OWF1) The description of f is publicly known and does not require any secret information for its operation.
(OWF2) Given x, it is easy to compute $f(x)$.
(OWF3) Given y, in the range of f, it is hard to find an x such that $f(x) = y$. Any efficient algorithm solving a P-problem succeeds in inverting f with negligible probability.

Zero-knowledge techniques [9] are mathematical methods used to verify things without sharing or revealing underlying data, and zero-knowledge protocols are probabilistic assessments. The goal is to prove a statement without leaking extra information, for example, for some N, x, prove x is a quadratic residue in Z_N^*.

Definition 7. Let $L \subseteq \Sigma^*$. A zero-knowledge proof system for L is a pair $(P,\ V)$ satisfying
(ZK1) For all $x \in L$, a verifier says "yes" after interacting with the prover (*Complete*);
(ZK2) For all $x \notin L$, and for all provers P^*, a verifier says "no" after interacting with P^* with probability at least 1/2 (*Sound*);
(ZK3) For all verifiers V^*, there exists a simulator S^* that is a randomized polynomial time algorithm such that for all $x \in L$,

$$\{transcript((P,\ V^*)(x))\} = \{S^*(x)\} \quad (Perfect). \tag{5}$$

3. Main results

Theorem 2. (WKDC law) *Let $G = \{p, q, x\}$ and let $(G, \bullet)$ is a public key group. Then*
(WKDC1) $x = x \bullet x = p \bullet q$ *and*
(WKDC2) $q = x \bullet q$ *iff* $x = 1$.

Proof. Assume (WKDC2) and prove (WKDC1). Let $p,\ q,\ x \in G$. Use the identities of group. The steps used to derive this identity

$$(p \bullet q) \bullet x = p \bullet (x \bullet q) = p \bullet q, \tag{6}$$

and

$$x \bullet (p \bullet q) = (x \bullet q) \bullet p = q \bullet p. \tag{7}$$

By Theorem 1, we have.

$$p \bullet q = q \bullet p, \tag{8}$$

and so

$$(p \bullet q) \bullet x = x \bullet (p \bullet q), \tag{9}$$

we deduce that

$$p \bullet q = x. \tag{10}$$

Since

$$x = p \bullet q = p \bullet ((p \bullet q) \bullet q) = (p \bullet q) \bullet (p \bullet q) = x \bullet x. \tag{11}$$

For (WKDC2). Let $q,\ x \in G$. By Definition 1. Define:

$$q \bullet q = 1, \tag{12}$$

we have

$$(x \bullet q) \bullet q = x \bullet (q \bullet q) = x \bullet 1, \tag{13}$$

and

$$q \bullet (x \bullet q) = (q \bullet q) \bullet x = 1 \bullet x, \tag{14}$$

and so

$$x \bullet 1 = 1 = 1 \bullet x, \tag{15}$$

Table 1: Table for $(G, \bullet)$.

$\bullet$	p	q	x
p	—	x	—
q	—	—	—
x	—	q	x

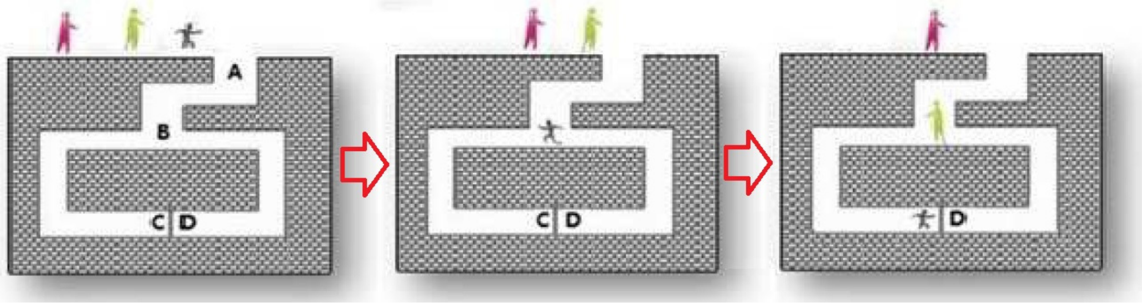

Figure 2:

Figure 1. Zero-knowledge proofs: An illustrated guide.

since $x = 1$, we deduce that

$$(x \bullet q) \bullet q = q \bullet (x \bullet q) = 1 \text{ implies } q = x \bullet q. \tag{16}$$

The verification of this identity is show in Table 1. □

Table 1 illustrates WKDC is a group and is to set up a stable algebra structure. Still, the outcome does not meet the distributive law and also does not meet associative law. It is this characteristic that provides a structure of security. The secret key is the corresponding value p (a large prime) such that $2^{200} \leq p \leq 2^{600}$. This should go without saying, but make sure you have a secure password q. To crack the code, the lottery is 2^{-200}. This $h(x)$ is a candidate for a one-way function. But until now, no probabilistic polynomial time algorithm is known that can invert $h(x)$, ever on a polynomial fraction of input.

It's also worth mentioning that the Theorem 2 gives another internal characterization of the WKDC law, that is — the problem of zero-knowledge proof of $n = p \bullet q$. Zero-knowledge cave, as shown in Figure 1.

Of course, in network to transmit news, except secrecy, the authentication, integrity and nonrepudiation are important to us. Here, we describe the multiplication function

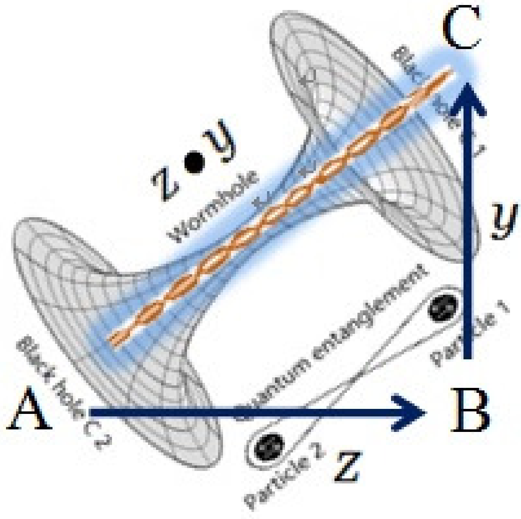

Figure 4:

Figure 2. The entanglement diagram of ($\{z,\ y\}$, $\bullet$).

that underlies the WCS. The following proposition is the "constructive" formulation of the fundamental theorem of groups.

Theorem 3. (Security of WCS) *A multiplication function $h(x,\ y,\ z)$ of a wormhole is a one-way function.*

Proof. Suppose G is a group of Pas (Ω) for all $x,\ y,\ z \in G$. Formally,

$$h(x, y, z) = (x \bullet y) \bullet z. \tag{17}$$

$h(x, y, z)$ is easy to compute when x, y and z are known, but $h(x, y, z)$ is hard to invert in the absence of x or y, or z. If x', y', $z' \in\ G$, inversion formula

$$\nexists h(x', y', z') = h(x, y, z) \text{ (or computationally hard).} \tag{18}$$

Let $\Lambda = \{0,\ 1\}$ and let $\lambda \in \Lambda'$. Define: $h(\lambda)$ is the string representing the product of the first and second halves of λ, we have

$$h(\lambda) = \lambda_1 \bullet \lambda_2, \tag{19}$$

where λ_1 is also the string representing the product of the first and second halves, that is

$$\lambda_1 = x \bullet y, \tag{20}$$

the string

$$\lambda = x \bullet y \bullet \lambda_2 \tag{21}$$

as binary numbers are $\{b_1, b_2, \cdots, b_k\}$.

If $|\lambda|$ is even, then

$$|\lambda_1| = |x \bullet y| = |\lambda_2|. \tag{22}$$

If $|\lambda|$ is odd, then

$$|\lambda_1| = |x \bullet y| = |\lambda_2| + 1. \tag{23}$$

Let $h(\lambda)$ is a compression function, i.e., $h(\lambda)$ is a fixed length and x or y, or λ_2 is any finite length. Then we need to pad $h(\lambda)$ with leading 0s so that it has the same length as λ. We deduce that cannot invert $h(\lambda)$(or $h(x,\, y,\, z)$). But it would technically — the probabilities of cheating by one of the penetrator are very small. □

Let p:$A \to B$ and $q : B \to C$. If $x : A \to C$ and $x = p \bullet q$, then p, q and x have a commutative diagram. Show that diagram is a valid commutative diagram ($x = z{\bullet}y$), i.e., quantum entanglement in wormhole, where x is a composite (or modulus), z and y be two large primes in Figure 2, and this is illustrated in Figure A1 (as noted in Appendix), we shows that the wormhole computation by the quantum entanglement method. Although our understanding of the wormhole of calculate is fairly limited, we use the design methodologies of algebra, i.e., the group is used to model the circuitry of electronic devices (e.g. analog multiplier) for simulates wormhole operations in identity (WKDC1). In fact, the quantum computers should be able to perform highly complex simulations. This identity (WKDC2) is implemented by the sick circuit, so it makes no operational sense. Obviously, this is an abstraction of mathematical concepts.

A public-key cryptosystem, such as RSA [10, 11], can be used to distribute private keys to pairs of individuals when they wish to communicate, and then use a private key system, such as data encryption standard (DES) [12] is a block cipher algorithm, for encryption and decryption of messages. About WKDC, it is best to use the WKD to avoid causing any damage the message (e.g. pion), just like a cloud storage. Wormhole computation is the basis for a method that can be used to perform arithmetic with large integers. More than that, wormhole teleportation is a jumping window, and it ensures integrality of messages, in particular to ensure opening of messages. In the WCS encryption method, messages are translated into sequences of integers. By the function expression of WCS, it follows that

(WCS1) $h(x,\, y,\, z) = f(x,\, y,\, z) \bullet g(x,\, y,\, z)$ and
(WCS2) $((x \bullet y) \bullet z) \bullet ((x \bullet z) \bullet y) = (z \bullet y) \bullet x$.

Definition 8. (Polynomial of WCS) Let $(X;\, \bullet, 1)$ is a BCL^+ algebra. Assume that for $a_n,\, a_{n-1},\, \cdots,\, a_0 \in X$, there is defined a coefficient $1x^i = 1$, and let $f(x) \in X[x]$ is a polynomial such that

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0. \tag{24}$$

Then $(X[x];\ \bullet,\ 1)$ is BCL^{+}algebra.

Definition 9. (Groups of WCS). Let G be a group for all $n, p, q \in G$. If

$$(f(p),\ g(q)) = 1. \tag{25}$$

Then

$$(h(n),\ f(p) \bullet g(q)) = 1. \tag{26}$$

We have
(WHT4) $h(n) = p\ \bullet\ q$,
where p and q be two large primes, n is a composite (200-digit for security).

4. Methods

First off, we needs to design the algorithms and mathematical details in order to further research about WCS.

4.1. Algorithm ($\mathcal{A}$)

// Using the current generation of computers for Algorithm ($\mathcal{A}$), because p and q be two large primes. //

• WCS parameter generation

***Step* 1**.

Generate two large primes, p and q, such that $p \neq q$, and generate one large number x.

***Step* 2**.

$\lambda \leftarrow pqx$ and $\phi(\lambda) \leftarrow (p-1)(q-1)(x-1)$.

***Step* 3**.

$e \leftarrow pq$.

***Step* 4**.

Choose a random m, such that $m^{*} \leftarrow me\lambda$, $\gcd(m,\ \phi(\lambda)) = 1$.

***Step* 5**.

// It is certainly necessary that λ must be large enough that factoring it will be computationally infeasible. //

The public key is $(\lambda,\ m^{*})$ and the private key is $(p,\ q,\ x,\ e)$.

• WCS encryption

***Step* 1**.

// The encryption key is kept secret. //

$f(p, q, n) = p.$

***Step* 2**.

// The encryption key is kept secret and send the secret message q of compression. //

$g(p, q, n) = q.$

***Step* 3**.

// The public-key is compression n and is release A in Figure A1. //

$h(p, q, n) = n.$

- **WCS decryption**

***Step* 1**.

// Receive the public-key of compression. //

$h(p, q, n) = n.$

***Step* 2**.

// Receive the secret message. //

$g(p, q, n) = q.$

***Step* 3**.

// The receiver uses the function expression to obtain the original message from its encryption, and this completes the algorithm. //

$f(p, q, n) = n/q = p.$

- **A ciphertext-only attack**

// Some attacks would receive the public-key n of compression. //

Design a factorization algorithm for n:
$h(p, q, n) = n = p \bullet q.$

As an application of group, consider the general case, the encryption and decryption are at a more complex organization than Algorithm $(\mathcal{A})$. We give the following algorithm for WCS.

4.2. Algorithm $(\mathcal{B})$

// It requires multi-multiplication tables of topological group, and by Definition 4 and Definition 5 for Algorithm $(\mathcal{B})$. //

***Step* 1**.

// Encryption key of WKDC. //

x, y, z.

***Step* 2.**

Some random data allocated from the WKDC and algebraic manipulation:

$h(x, y, z) = (z \bullet y) \bullet x = \lambda$.

***Step* 3.**

// Public-key λ. //

$h\ (\lambda) = \lambda$.

***Step* 4.**

Alice and Bob have common encryption key:

$h\ (e) = (x \bullet z) \bullet y = e$.

***Step* 5.**

Alice's encryption key:

$d = (x \bullet y) \bullet z$.

***Step* 6.**

// Alice and Bob need to be assured that the λ is true. //

$d \bullet e = \lambda$.

***Step* 7.**

// By Definition 5 and (WCS2). //

Check the encryption key:

$((x \bullet y) \bullet z) \bullet ((x \bullet z) \bullet y) = (z \bullet y) \bullet x$.

***Step* 8.**

A numeric λ release by Alice.

***Step* 9.**

// Non-repudiation!! //

Digital signature: A numeric e transfer from Alice to Bob.

***Step* 10.**

A plaintext m by Bob.

***Step* 11.**

// Attack, this hope is forlorn. //

Bob's ciphertext:

$m^* = (m \bullet e) \bullet \lambda$.

***Step* 12.**

A ciphertext m^* transfer from Bob to Alice.

***Step* 13.**

Alice decryption:

$m = (m^* \bullet\ e) \bullet d$.

Table 2: BCL^+ operations • of ({1, x, y, z}) for both encryption and decryption.

$\bullet$	1	x	y	z
1	1	1	1	1
x	x	1	1	z
y	y	1	1	z
z	z	1	z	1

Remark 1. The relation between d and λ is that they are mutually multiplicative BCL^+ algebras, meaning that

$$\lambda \bullet d = 1 = d \bullet \lambda \quad \text{implies} \quad m = m^*/e \bullet \lambda. \tag{27}$$

Remark 2. Algorithm ($\mathcal{B}$) illustrates how WCS based on the topological group and BCL^+algebras encryption and decrypt the messages are performed. And most of all, even after leaked three numeric m^*, e and d once, this result affect only this once, the system security remains the same because WCS is a formidable system. In the new algorithm, a central feature is multivariate WCS. The algorithm provides that the algorithmic mechanism for identifying the invader. Moreover, the quick Algorithm ($\mathcal{B}$) only shows how to multiplication. (Wormhole computer is very good at, but with that also lead to headaches of God.)

Remark 3. Elementary aspects of security. The hard task here is factorization of large integers λ into primes y, z and x (x need not be prime). WCS has four private keys, that is y (or prime p), z (or prime q), x, and e. In comparison, RSA has three private keys, that is p, q, and a.

Remark 4. The most obvious advantage of speed of encryption/decryption algorithms is to calculate very quickly. In comparison, both the encryption and the decryption operations in the RSA cryptosystem are modular exponentiations.

We illustrate the application of the above algorithm with an example.

Example 1. Suppose Alice chooses $x = 101$, $y = 113$ and $z = 227$. Then $\lambda = 2590751$. Both y and z are primes. Alice publishes $\lambda = 2590751$ and keeps x, y and z secret. She computes the encryption key e, by the following Cayley Table 2.

$e = 227 \times 113 = 25651$. Then Alice transmits to Bob 25651. Whenever Bob wants to send Alice a secure message, for example, $m = 9726$, he computes the plaintext

$$m^* = 646344772041126.$$

He transmits this to Alice. When Alice receives such a message, she decrypts by computing

$$m = \frac{m^*}{e \times \lambda} = 9726. \tag{28}$$

We conclude that we have determined the correct key. □

Implementing the WCS, let's now do an example to illustrate encryption and decryption. Obviously, this construction generalizes Example 1.

Example 2. Here, we describe the one-way function that underlies the WCS cryptosystem. We give its associated trio f, M, and h. The generator machine M operates this Example 1. Doing so is possible because the set of numbers $\{1, \cdots, \phi(\lambda)\}$ that are relatively primes to $\phi(\lambda)$ form a group under the operation of BCL multiplication $\phi(\lambda)$. It selects a random number m, and he index to the function f consists of the four numbers x, y, z and m. Finally, the algorithm computes the multiplicative inverse d. M outputs $((\lambda, m), d)$, where $d = e \times \lambda$. Function h properly inverts because $h(d, f_{\lambda,m}) = h_d(f_{\lambda,m})$ for any m and λ. So, h properly inverts f, we says that $f_{\lambda,m}$ is hard to invert in the absence of e. □

5. Principles

Is the WCS really Vernam (or One-Time Pad (OTP))? In other words, we will give the security proof for WCS. First, we have the following design principles.

Principle 1. The key not reuse and wonderful key quality (i.e., the WCS is unbreakable when used properly).

Principle 2. In WCS, the next random bit is inscrutable.

Principle 3. The plaintext of WCS that a same character uses the multi-multiplication tables can make a significant difference in the outcome of the encryption.

Principle 4. The ciphertext (e.g., ciphertext m^* of WCS in Algorithm ($\mathcal{B}$)) does not make sense and random to put a bunch of text private menus, including the nonprintable characters of the ASCII.

Remark 5. In fact, the OPT is symmetrical. But WCS is a brand-new OPT, is unsymmetrical.

Theorem 4. (Unsymmetrical WCS). *Let E be an encryption sets and let D be a decryption sets. Then $E \not\Leftrightarrow D$.*

Proof. Let λ is the public-key, by Algorithm ($\mathcal{B}$), we know that

$$d \bullet e = \lambda \tag{29}$$

must be BCL^{+} algebraic over Y [7, 8] [13, 14] [15, 16]. Certainly

$$\nexists\, e^{-1} \text{ implies } \nexists\, \mathrm{d} = \lambda \bullet \mathrm{e}^{-1} \text{ (Bob cannot count } d\text{).} \tag{30}$$

Working in Algorithm ($\mathcal{B}$), we find this decryption key d is unsymmetrical algebraic structure, that is

$$d \bullet e \neq e \bullet d. \tag{31}$$

We have $e \in E$ and $d \in D$. So, we deduce that $E \nRightarrow D$ and $E \nLeftarrow D$. □

6. Conclusions

The research presented above focuses on the creation and implementation of the WCS. We have successfully introduced a new mathematical tool, and named the groups for proving secure wormhole public-key cryptosystems. Unlike other encryption key solutions, due to this Algorithm ($\mathcal{B}$) that utilizes an unsymmetrical algebraic structure will be a feature of cryptography. No doubt, the concept of wormhole come from cosmology, and is related to quantum entanglement, which we find to be an important topic. But more importantly, we can use two wormholes for physical background of cryptography or we can also leave it encryption. Studies on these topics are not only providing rich scientific insight in terms of new physics but also potentially have important long-term technological implications, including the development of cryptosystems that support quantum communication are immune to safety, are robust against feature guaranteed unidirectional transmission (or a one-way function). To construct an encrypted form which has the required properties, and to prove that it has these properties, is a purely algebraic task. It should be interesting algebraic cryptograms and may represent a trend in the future. The reader is invited to consider the direction for wormhole cryptography.

7. Appendix

The particles of entanglement in the two wormholes, as shown in the following Figure A1 (see [4]).

Acknowledgements

The author is grateful to the anonymous referees for useful comments and suggestions.

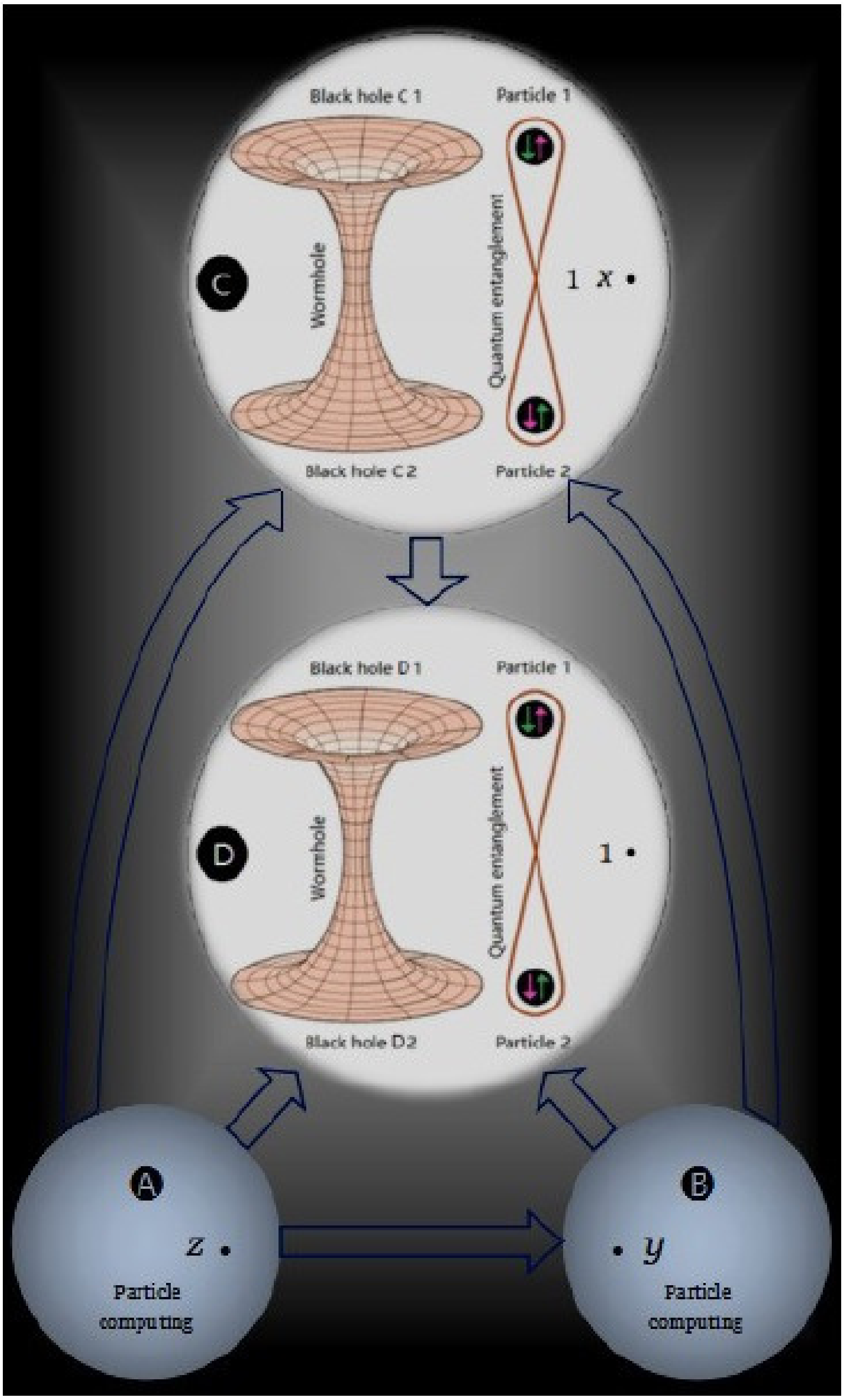

Figure A1. Two wormholes of WCS. *Figure credit:* Y. Liu, 2019, *IJCAA*, 1, 33.

References

[1] van Raamsdonk, M.: Building up spacetime with quantum entanglement. Gen. Rel. Grav. 42, 2323-2329, (2010). https://doi.org/10.1142/S0218271810018529

[2] Maldacena, J., Susskind, L.: Cool horizons for entangled black holes. Fortsch. Phys. 61, 781-811, (2013). https://doi.org/10.1002/prop.201300020

[3] Ron, C.: The quantum source of space-time. Nature. 527(16), 290-293, (2015). https://doi.org/10.1038/527290a

[4] Yonghong, L.: New groups to ER = EPR conjecture. International Journal of Cosmology, Astronomy and Astrophysics. 1(1), 33-37, (2019).

[5] Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In Proc. 35th Ann. Symp. Foundations of Computer Science. IEEE Press, pp 124-134, (1994).

[6] Diffie, W., Hellman, M.E.: Multiuser cryptographic techniques. In Proc. AFIPS National Computer Conference, pp 109-112, (1976).

[7] Yonghong, L.: On BCL^+-algebras. Advances in Pure Mathematics. 2(1), 59-61, (2012). https://doi.org/10.4236/apm.2012.21012

[8] Yonghong, L.: Topological BCL^+-algebras. Pure and Applied Mathematics Journal. 3(1), 11-13, (2014). https://doi.org/10.11648/j.pamj.20140301.13

[9] Goldwasser, S., Micali, S., Rackoff, C.: The knowledge complexity of interactive proof systems. In Proc. 17th ACM Symposium on Theory of Computing, pp 291-304, (1985).

[10] Diffie, W., Hellman, M.E.: New directions in cryptography. IEEE Trans. Info. Theory. IT-22(6), 644-654, (1976).

[11] Merkle, R.C.: Secure communication over insecure channels. Communications of the ACM. 21(4), 294-299, (1978).

[12] Coppersmith, D.: The data encryption standard (DES) and its strength against attacks. IBM Journal of Research and Development. 38, 243-250, (1994).

[13] Yonghong, L.: Filtrations and deductive systems in BCL^+ algebras. British Journal of Mathematics & Computer Science. 8(4), 274-285, (2015). https://doi.org/10.9734/BJMCS/2015/15901

[14] Yonghong, L.: Liu's laws and p-BCL^+ algebras. International J. of Pure & Engg. Mathematics. 3(II), 51-58, (2015).

[15] Yonghong, L.: Standard ideals in BCL^+ algebras. Journal of Mathematics Research. 8(2), 37-44, (2016). https://doi.org/10.5539/jmr.v8n2p37

[16] Yonghong, L.: *pa*-BCL^+ Algebras and Groups, Applied Mathematics & Information Sciences. 3(11), 891-897, (2017). https://doi.org/10.18576/amis/110329