



- (51) **International Patent Classification:** Not classified
- (21) **International Application Number:**
PCT/MY2010/000190
- (22) **International Filing Date:**
30 September 2010 (30.09.2010)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
PI 20094827 13 November 2009 (13.11.2009) MY
- (71) **Applicant (for all designated States except US):** **MIMOS BERHAD** [MY/MY]; Technology Park Malaysia, 57000 Kuala Lumpur (MY).
- (72) **Inventors; and**
- (75) **Inventors/Applicants (for US only):** **MAJEED, Mohammed, Munther, A.** [IQ/MY]; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **AL-KHATEEB, Khalid, A., S.** [IQ/MY]; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **SAEB, Magdy, M.** [EG/MY]; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **WAHID-DIN, Mohamed, Ridza** [MY/MY]; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY).
- (74) **Agent:** **MIRANDAH, Patrick;** Patrick Mirandah Co. (Malaysia) SDN BHD, Suite 3B-19-3 Plaza Sentral, Jalan Stesen Sentral 5, 50470 Kuala Lumpur (MY).

(81) **Designated States** (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) **Designated States** (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))

Published:

— without international search report and to be republished upon receipt of that report (Rule 48.2(g))

(54) **Title:** A SECURE KEY DISTRIBUTION PROTOCOL BASED ON HASH FUNCTIONS UTILIZING QUANTUM AUTHENTICATION CHANNEL (KDP-6DP)

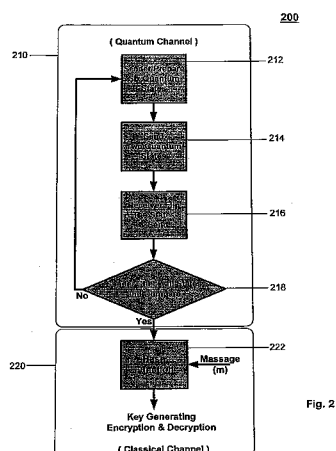


Fig. 2

(57) **Abstract:** A method for a secure key distribution protocol based on hash functions utilizing quantum authentication channel (KDP-6DP) (200), comprising authenticating (210) a receiver using quantum authentication channel and distributing (220) secure key from sender to the receiver by encrypting message using hash functions (222). Authenticating the receiver using quantum authentication channel further comprises preparing six quantum states at a sender (212), sending two quantum states to the receiver (214), flipping the quantum states at the receiver (216), sending back the flipped quantum states to the sender (216), and validating the quantum states at the sender (218).

A SECURE KEY DISTRIBUTION PROTOCOL BASED ON HASH FUNCTIONS UTILIZING QUANTUM AUTHENTICATION CHANNEL (KDP-6DP)

FIELD OF INVENTION

5

The present invention relates generally to a method for a secure key distribution protocol based on hash functions utilizing quantum authentication channel.

BACKGROUND ART

10

Key distribution is a fundamental process in cryptography applications either in symmetric or asymmetric ciphers. In symmetric ciphers, one usually resorts to a courier-based key exchange or in some cases quantum key distribution is used. On the other hand, a schema for using hash functions as a medium for key exchange in both symmetric and asymmetric cipher allows the data to be encrypted and decrypted in a secure form.

15

20

25

Patent No US 5729608 (Janson et al.) discloses a method and system for providing secure authenticated cryptographic key distribution in a communication system wherein having properties similar to a Two-Party Authentication Protocol. However, the prior article is distinguished from the present invention in that it only teaches a protocol of key distribution and authentication that is similar to the Two-Party Authentication Protocol. The protocol does not teach any method of key distribution using hash functions and a random string. It has a disadvantage in that it may not protect against any eavesdroppers and other data attacks. The present invention allows the sender and/or receiver to detect any data transmission attack if there are any occurrences of such trespassing. Moreover, the message passes through several encryption and character authentication processes that are not available in the prior art above. Therefore, the present invention has disclosed a novel protocol of key

distribution based on hash functions and utilizing an authentication channel for the enhancement of security in key distribution.

In another patent which is patent No US 5515438 (Bennet et al.), that discloses a quantum
5 key distribution. It uses non-orthogonal quantum states to distribute random information. However, the prior art has a disadvantage wherein the key is merely transmitted by applying quantum cryptography which is said to be insecure. With current advancement of technology, eavesdropping and other advance data attackers may easily intercept the transmission of data in the quantum channel. Therefore, by applying additional hash function
10 ciphering and deciphering in quantum channel, the present invention introduces a new protocol in key distribution and message encryption towards this process.

The present invention seeks to address the above-mentioned disadvantages over the prior arts by promoting novel and inventive protocol generate a secure key distribution based on
15 hash functions and utilizing quantum authentication channel. The present invention introduces high security and reliability in preserving the transmission of secure message and data as compared to prior arts.

SUMMARY OF INVENTION

One object of the invention is to provide a method for a secure key distribution protocol based on hash functions utilizing a quantum authentication channel. The method comprises authenticating a receiver using quantum authentication channel and distributing secure key from the sender to the receiver by encrypting message using hash functions. Authenticating the receiver using quantum authentication channel further comprises preparing six quantum states at a sender, sending two quantum states to the receiver, flipping the quantum states at the receiver, sending the flipped quantum states to the sender and validating the quantum states at the sender.

Preferably, the quantum authentication channel is an out-of-band channel and comprises a free space or optical fiber. Preferably, the two quantum states comprise sending two qubits.

Another object of the invention is where flipping the quantum states comprises using one of four operators of I , X , iY or Z and, validating the quantum states that includes testing forward and backward paths of the quantum channel.

A further object of the present invention is where the hash functions includes selected hash or a cascade of hash functions and shared secret keys and preferably, the secure key comprises either first mode of key distribution using random string between the sender and the receiver; or second mode of key distribution using one string at sender station, and third mode of key distribution using one string generated, message encryption and concatenation at sender station, and send to receiver station to get the value of j for driving the hash cascade selection and get the key and message.

The present invention consists of features and a combination of parts hereinafter fully described and illustrated in the accompanying drawings, it is being understood that various

changes in the details may be made without departing from the scope of the invention or sacrificing any of the advantages of the present invention.

BRIEF DESCRIPTION OF THE ACCOMPANYING DRAWINGS

To further clarify various aspects of some embodiments of the present invention, a more particular description of the invention will be rendered by references to specific embodiments thereof, which are illustrated, in the appended drawings. It is appreciated that these drawings depict only typical embodiments of the invention and are therefore not to be considered limiting of its scope. The invention will be described and explained with additional specificity and detail through the accompanying drawings in which:

- 10 FIG. 1 is data flow of a secure key distribution protocol based on hash functions utilizing quantum authentication channel using deterministic six state protocol (KDP-6DP).

FIG. 2 is a flow chart of quantum authentication process using quantum authentication channel and key distribution based on hash functions.

15

FIG. 3 is a flow chart of a first mode of key distribution using random string between a sender and a receiver.

20

FIG. 4 is a flow chart of a second mode of key distribution using one string generated at a sender.

FIG. 5 is a flow chart of a third mode of key distribution using one string generated, message encryption and concatenation at a sender. and send to receiver station to get the value of j for driving the hash cascade selection and get the key and message.

25

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention relates to a method for a secure key distribution protocol based on hash functions and utilizing quantum authentication channel. Hereinafter, this specification
 5 will describe the present invention according to the preferred embodiments of the present invention. However, it is to be understood that limiting the description to the preferred embodiments of the invention is merely to facilitate discussion of the present invention and it is envisioned that those skilled in the art may devise various modifications and equivalents without departing from the scope of the appended claims.

10

The method for a secure key distribution protocol according to the present invention comprises authenticating (210) a receiver using quantum authentication channel and distributing (220) secure key from sender to the receiver by encrypting message using hash
 15 functions (222). Authenticating the receiver using quantum authentication channel further comprises preparing six quantum states at a sender (212), sending two quantum states to the receiver (214), flipping the quantum states at the receiver (216), sending the flipped quantum states to the sender (216), and validating the quantum states at the sender (218).

FIG. 1 depicts a flow data diagram of a secure key distribution protocol based on hash
 20 functions utilizing six-state quantum authentication channel (100). In the first stage, the sender prepares two qubits (144) rather than one of the six states given by equations (1), (2), and (3) wherein the equations as shown below:

$$\begin{aligned} \hat{z} = Z &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, & \hat{x} = X &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \\ 25 \quad \hat{y} = Y &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \end{aligned}$$

and their respective eigenvectors:

$$|z+\rangle = |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |z-\rangle = |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad (1)$$

$$|x\pm\rangle = (|z+\rangle \pm |z-\rangle) / \sqrt{2}, \quad (2)$$

$$|y\pm\rangle = (|z+\rangle \pm i|z-\rangle) / \sqrt{2}, \quad (3)$$

5

At the sender station (140), the sender delivers the two qubits to the receiver station (120) through quantum authentication channel (130), wherein the quantum channel consists of free space or optical fiber. The quantum channel is an out-of-band channel wherein eavesdropper or any other data attacks may not intercept. This channel provides security and confidentiality of the characters transmitted from the sender (140) to the receiver (120).

10

Upon receiving the two qubits, the receiver (120) then performs qubits flipping process (124) by operating the qubits with one of the four operators I , X , iY or Z . This would result in zero, one or two qubits being flipped, as shown in Table 1 below.

15

Table 1

Sender's Basis' Choice	X	iY	Z	I
$\hat{x} \hat{y}, \hat{y} \hat{x}$	1	1	2	0
$\hat{x} \hat{z}, \hat{z} \hat{x}$	1	2	1	0
$\hat{y} \hat{z}, \hat{z} \hat{y}$	2	1	1	0
Boolean value	10	01	11	00

Table 1 shows that the possible combinations of the qubits send back by the receiver (120), the operations on the qubits and the qubits flipping process (124) as result of the measurement by the receiver (120).

20

Subsequently, after performing qubits flipping process (124) by using one of the I , X , iY or Z operators, the flipped qubits are resent to the sender (140) to be measured in the same

basis where they were prepared in, thus letting the sender (140) decide deterministically how many qubits had been flipped by the receiver (120).

Thereafter, the receiver (120) resends both the flipped qubits to the sender (140) to re-
 5 measure the flipped qubits. In authentication, the operators chosen by the receiver (120) or sender (140) are the same as they expect the outcomes of their measurement to be correlated on both the forward and backward paths. Every deviation from this anticipated scenario is considered an error. If the detected errors are below a certain security threshold, established in advance by the sender (140) and receiver (120), the communication goes on
 10 with the usual error correction and privacy amplification stages. However, if the security threshold is transcended, the whole communication aborts.

In ensuring secure data transmission against eavesdropper attacker (Eve), sender (140) and receiver (120) forfeit the run to perform quantum channel control. The sender (140) and
 15 receiver (120) test the forward and backward paths of the channel with a procedure equivalent to the one adopted in BB84 protocol. Upon receiving the two qubits from sender (140), the receiver (120) makes a projective measurement of the two qubits along a basis randomly chosen among $\hat{x}$, $\hat{y}$ or $\hat{z}$. The sender (140) authenticates the receiving part is the designated receiver (120).

20

For the first example, when sender (140) sends qubits in the $\hat{x}, \hat{y}$ combination by choosing the states $|x+\rangle$ and $|y+\rangle$ and if the sender's (140) final measurements results in none or both of the qubits flipped in the qubits flipping process (124), sender (140) would assume that the operation handled by the receiver (120) was using the $I(Z)$ operator.

25

For a second example, sender (140) authenticates that the designated receiver, also if it results in the only state $|x+\rangle (|y+\rangle)$ flipped, the operator used is $iY(X)$.

Once the sender (140) has authenticated that the receiver (120) is the designated receiver (120) to receive the data, the sender proceeds with message encryption (142) at his/her particular station (140). In this stage, the hash functions (142,122) wherein consists of at least selected hash cascade of two hash functions is used to cipher and decipher the message. After encryption (142) is performed at the sender's station, the ciphered message is transmitted through classical channel or the Internet (110). During this particular process, 10 eavesdropper and other malicious attacks may not be able to intercept the transmission as the message has been encrypted by the hash functions and the receiver has primarily been authenticated. In result of the sender (140) and receiver (120) authentication, which has previously performed in the quantum channel, the message may be straightforwardly delivered to the legitimate receiver. The encrypted message is then transmitted to the 15 receiver station (140) for the receiver to decrypt (122) and retrieve the message.

The key distribution protocol is performed by atomic actions as in Table 2 by the sender and the receiver:

Table 2

Action	Form	Informal Implication
Send	$\langle m : A \rightarrow B \rangle$	Send message m from A to B
Receive	$(m : A \rightarrow B)$	Receive message m from A at B
New	$(v\ j)$	Obtain new value of j
Concurrently execute	$\otimes$	Cluster can be executed concurrently
Sequentially execute	$;$	Sequential or ordered actions
Concatenate	$S_x S_y = (S_x \parallel S_y)$	Strings S_x and S_y are concatenated into one string $S_x S_y$
Encrypt	$E_k(m) = C_m$	Encrypt message m using key k to get cipher C_m

Decrypt	$D_k(C_m) = m$	Decrypt cipher C_m using key k to get message m
Logical XOR	$\oplus$	Perform logical XOR between two variables
Halt	.	Stop execution of protocol
Generate	$\Rightarrow S_A$	Generate a random string S_A
Get	$\Leftarrow j:$	Get the value of j
Assigned to	$:=$	A value is obtained from an operation on the right hand side
Obtained from	:	A value is obtained from an indicated procedure
Value from a field	$\leftarrow [K_{sA}]$	Get a value of a variable from a certain field in K_{sA}
Wait	!	Wait for a message

Referring to FIG. 1, the figure explains the basis of the present invention pursuant to FIG. 2 of a protocol to generate a secure key distribution based on has functions utilizing quantum authentication channel (200). In the first stage of authenticating (210) the receiver, the sender prepares six quantum states (212) and sends two quantum states (214) to the receiver. The receiver then flips the states and sends (216) to the sender to check and compare (218) whether all states corresponds with what the receiver has flipped. This process continues with its forward and backward paths until the measurement by the receiver and the sender corresponds. If the flipped state does not correspond, the process restarts from the first stage of preparation of the six quantum states (212). This is to ensure that the receiver is a legitimate receiver. Then, in key distribution (220) process, once after the receiver is authenticated in the quantum channel, the sender sends the encrypted message using hash functions (222) through classical channel to the receiver for decryption. This secure distribution allowed the message to be securely transmitted from one sender to designated receiver.

Referring to Table 3 and FIG. 3 depict the first mode of key distribution by using random string (300) between a sender, Alice and a receiver Bob.

Table 3

Alice	Bob
$\Rightarrow S_A$	$\Rightarrow S_B$
$\langle S_A, A \rightarrow B \rangle \otimes (S_B, B \rightarrow A)$	$\langle S_B, B \rightarrow A \rangle \otimes (S_A, A \rightarrow B)$
$(\Leftarrow j, K_A, S_A \oplus S_B)$	$(\Leftarrow j, K_B, S_A \oplus S_B)$
$\langle K_A, A \rightarrow B \rangle \otimes (K_B, B \rightarrow A)$	$\langle K_B, B \rightarrow A \rangle \otimes (K_A, A \rightarrow B)$
IF $(K_A \neq K_B)$ then Abort	IF $(K_B \neq K_A)$ then Abort
Else $(\Leftarrow j, (v_j) \leftarrow [K_A])$	Else $(\Leftarrow j, (v_j) \leftarrow [K_B])$
$(\Leftarrow \text{Key}(A, K_{AS} = h_1(\alpha, \beta, \gamma, K_A)))$	$(\Leftarrow \text{Key}(B, K_{BS} = h_1(\alpha, \beta, \gamma, K_B)))$

In the Alice station (348), Alice generates S_A (346) to generate a string. S_B string is also generated in Bob station (310) on the concurrent time. These generated strings will be cross-distributed in a random mode to Alice station (348) and Bob station (310) respectively. Alice (348) and Bob (310) perform the following operation of $K_s = S_A$ or S_B (340, 318) where K_s is the sub-key used only for verification. However, the only restriction on these two random strings (S_A and S_B) is that their length (L), in number of bits, should be greater than or equal to the required key length pointer field given by n_K . That is $L_{SA}, L_{SB} \geq n_K$. In general L_{SA} and L_{SB} do not have to be equal in length. First n_K bit is used as the sub-key K_s and the bits of the secret field, in this sub-key, as a pointer to the hash function is utilized. The size of K_s is taken the same as the length of the smaller string.

Next, both Alice (348) and Bob (310) exchange the sub-key of K_{SA} to Bob (338) and K_{SB} to Alice (320) to verify its correctness and that no transmission errors occurred while exchanging S_A and S_B . Considering the value of K_s as an initial value (h_0) to a pseudo random number generator (PNRG), now Alice (348) and Bob (310) independently can perform, on site, the following operation:

$$h_{i+1} = h(a_i * h_i + b_i),$$

where a_i and b_i are both elements of a set of large random integers that is a part of the shared secret between Alice (348) and Bob (310) and $i = 0, 1, 2, \dots, n$. The initial vector (IV) of the hash h is also part of this shared secret. This set of constants and the vector IV can be

generated from a physical device acting as a true random number generator and stored for further use. This addition of random variables to the computation of the pad using hash function tends to approximate the behavior of a true random number generator. The values of the constants and the vector IV should be changed regularly, however not for every session.

The size of the required key (K) is determined by n,

$$\text{where } n = \left\lceil \frac{\text{requiredkeysize}}{\text{hashwordsize}} \right\rceil \text{ bits}$$

- 10 Alice (348) or Bob (310) can select a different hash every time a new session is started. The hash is selected from a value in a secret field of the sub-key K_S .

After both of the receiver and sender, Alice (348) and Bob (310) received K_{SA} and K_{SB} respectively (322, 336), they will compare $K_{SA}=K_{SB}$ and $K_{SB}=K_{SA}$ (334, 324) to check whether both the keys corresponds with each other in order to verify whether the sender and the receiver are legitimate parties. Once verified, the process proceeds to encryption and decryption of message (330, 328) wherein the message will be transmitted either to Alice station (348) or Bob station (310) through classical channel or internet.

- 20 Referring to Table 4 and FIG. 4 shows a flow chart of a second mode of key distribution using one string generated at a sender, Alice station (400).

Table 4

Alice	Bob
$\Rightarrow S$	$\Rightarrow S$
$\Rightarrow S_A(A \rightarrow B)$	$\Rightarrow S_B(A \rightarrow B)$
$(\Rightarrow H(G)) = [S_A]$	$(\Rightarrow H(G)) = [S_B]$
$(\Rightarrow Key(A, K_A = H((\alpha, \beta, G, S_A)))$	$(\Rightarrow Key(B, K_B = H((\alpha, \beta, G, S_B)))$

This is a different mode that may be applied in order to distribute key from Alice station (432) to Bob station (410). In this mode, Alice generates string S_A (430) and sends S_A to Bob (428). Concurrently, Bob waits (412) without generating his own string. Both Alice (432) and Bob (410) read the value of j (426, 416) that is the pointer to the type of hash to be employed.

- 5 Further, both of the sender and receiver perform $(K) = h_j(\alpha, \beta, \zeta, V_j, K_{AS} \text{ or } K_{BS})$ (424, 418). Next, the obtained key is encrypted (422, 420) in Alice (432) and Bob (410) stations by using hash functions and transmitted to each other for message retrieval. The value of j may be used to choose random combinations of two cascades hash function stored.

The example of the selected hash is shown below:

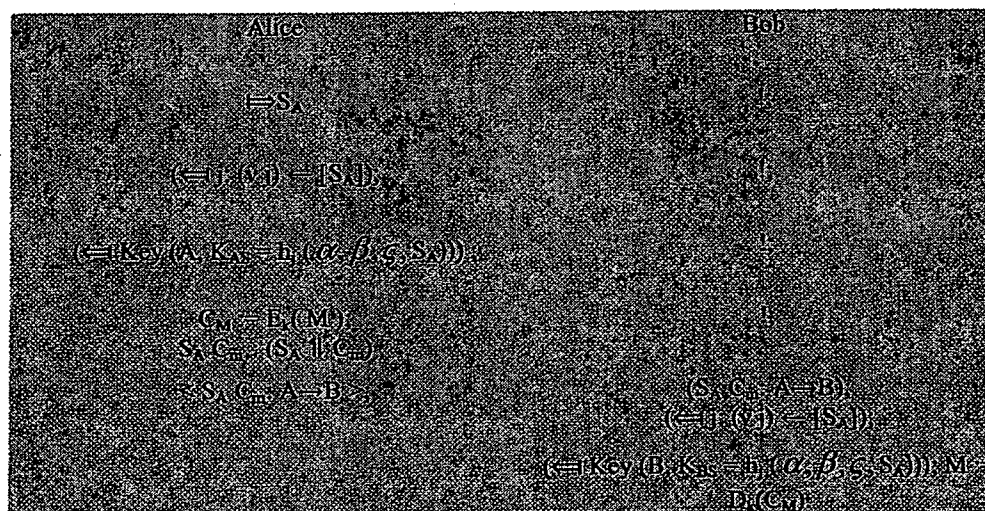
j	Sample selection of cascaded Hash functions
0	h_2, h_4
1	h_3, h_1
2	h_7, h_0
3	h_6, h_5
4	h_4, h_2
5	h_0, h_3
6	h_1, h_6
7	h_5, h_7

10

Referring to Table 5 and FIG. 5 shows a flow chart of third mode of key distribution (one shot) using one string generated, message encryption and concatenation at sender's station and sent to the receiver, Bob station for message retrieval (500).

Table 5

15



Alice (542) generates S_A (540) and get value of j (V_j), A from S_A (538). Then Alice (542) performs $(A, K_{AS} = hj(\alpha, \beta, \zeta, S_A))$ (536) to generate a key. The key generated is encrypted in a character of $C_M = E_k(M)$ (534). Once encrypted, the characters are concatenated (532) by performing $S_A C_M = (S_A C_M)$ (532). Alice then sends $S_A C_M$ (530) to Bob for authentication. Bob
 5 then receives $S_A C_M$ (522) to get j (V_j) from S_A (524) and performs $(K_{BS} = hj(\alpha, \beta, \zeta, S_A))$ (526) to generate a new key. Finally, message is retrieved at Bob's station as $M = D_k(C_M)$ (528). During generation of key (540) at Alice station (542), Bob has to wait (512, 514, 516, 518, 520) until a specified generated key has been established.

10 Since other modifications and changes varied to fit particular operating requirements and environments will be apparent to those skilled in the art, the invention is not considered to be limited to the example chosen for purposes of disclosure, and covers all changes and modifications which do not constitute departures from the true scope of this invention.

15 Having thus described the invention, what is desired to be protected by this patent is presented in the subsequently appended claims.

CLAIMS

1. A method for a secure key distribution protocol based on hash functions utilizing quantum authentication channel (200) comprising:

5 authenticating (210) a receiver using quantum authentication channel; and
distributing (220) secure key from sender to the receiver by encrypting message using hash functions (222);

characterized in authenticating (210) the receiver using quantum authentication channel further comprises:

10 preparing six quantum states at a sender (212);
sending two quantum states to the receiver (214);
flipping the quantum states at the receiver (216);
sending the flipped quantum states to the sender (216); and
validating the quantum states at the sender (218).

15

2. The method according to claim 1 wherein the quantum authentication channel is an out-of-band channel.

3. The method according to claim 1 wherein the quantum authentication channel
20 comprises a free space or optical fiber.

4. The method according to claim 1 wherein sending the two quantum states (214) comprises sending two qubits.

25 5. The method according to claim 1 wherein flipping the quantum states (216) comprises using one of four operators of I, X, Y or Z to flip the quantum states.

6. The method according to claim 1 wherein validating the quantum states (218) includes testing forward and backward paths of the quantum channel.

7. The method according to claim 1 wherein hash functions (222) includes selected
5 hash or a cascade of hash functions and shared secret keys.

8. The method according to claim 1 wherein distributing (220) the secure key comprises:

either first mode of key distribution using random string between the sender and the
10 receiver;

or second mode of key distribution using one string at sender station;

or third mode of key distribution using one string generated, message encryption and concatenation at sender station.

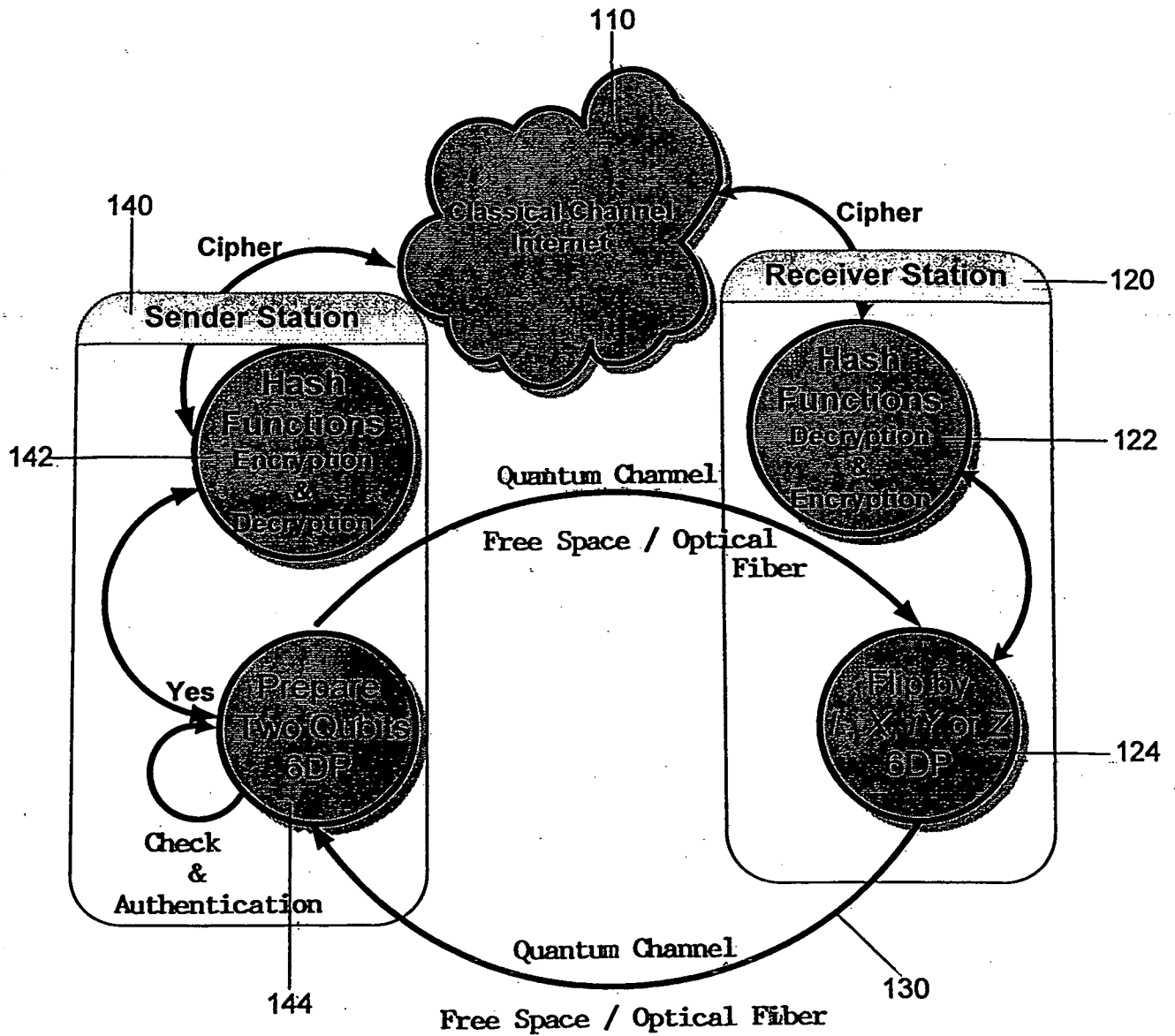
100

Fig. 1

2/5

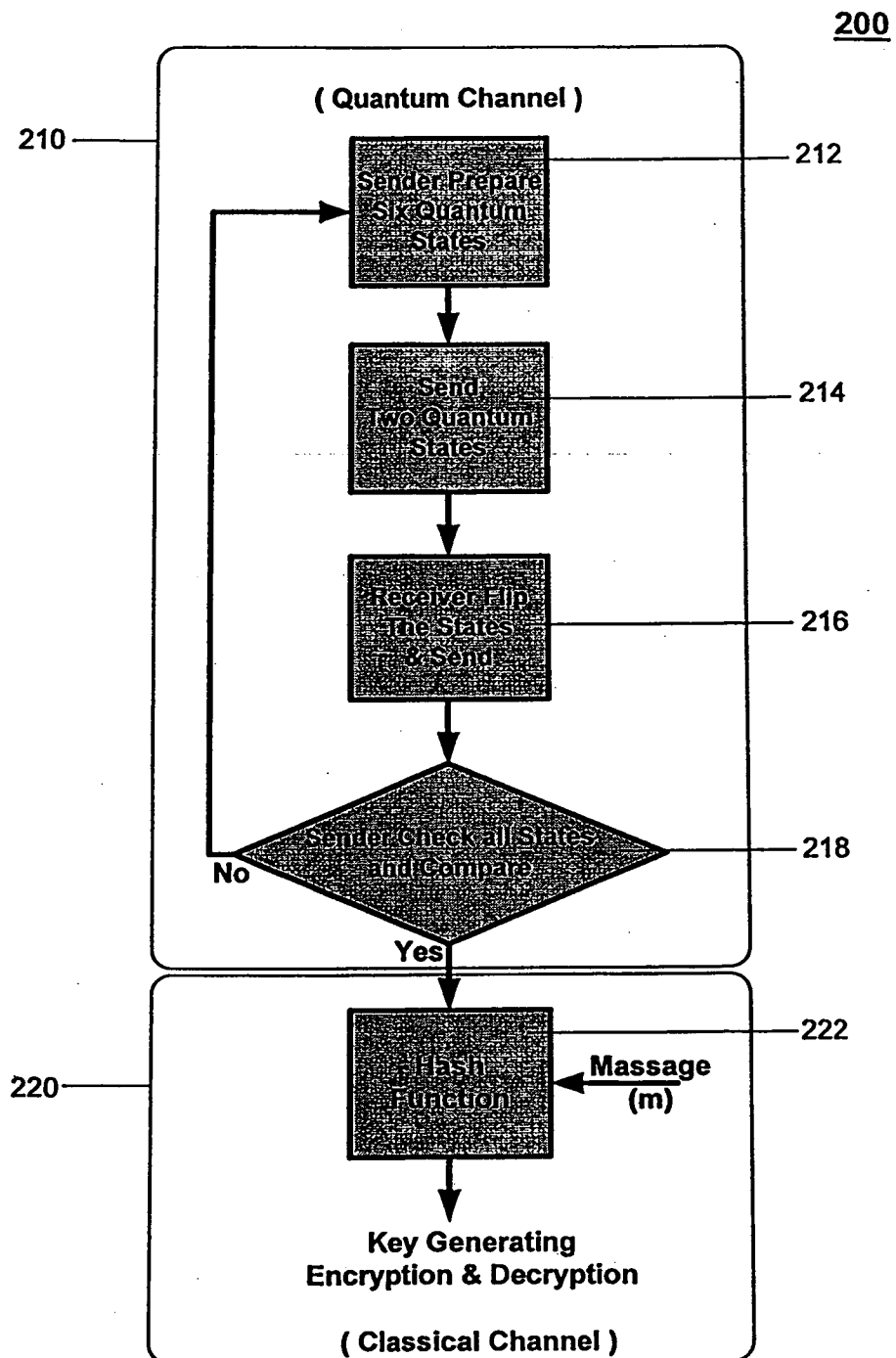


Fig. 2

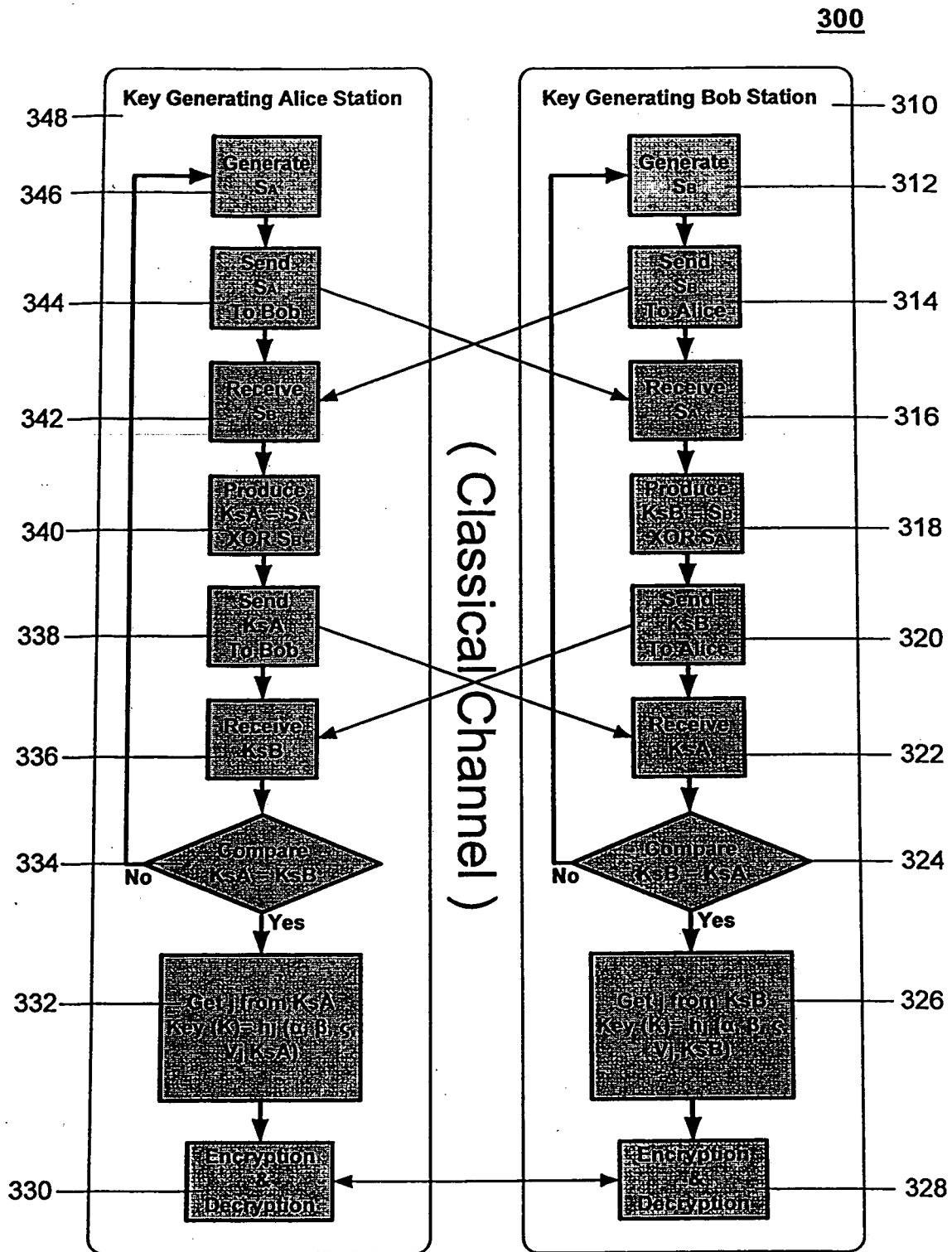


Fig. 3

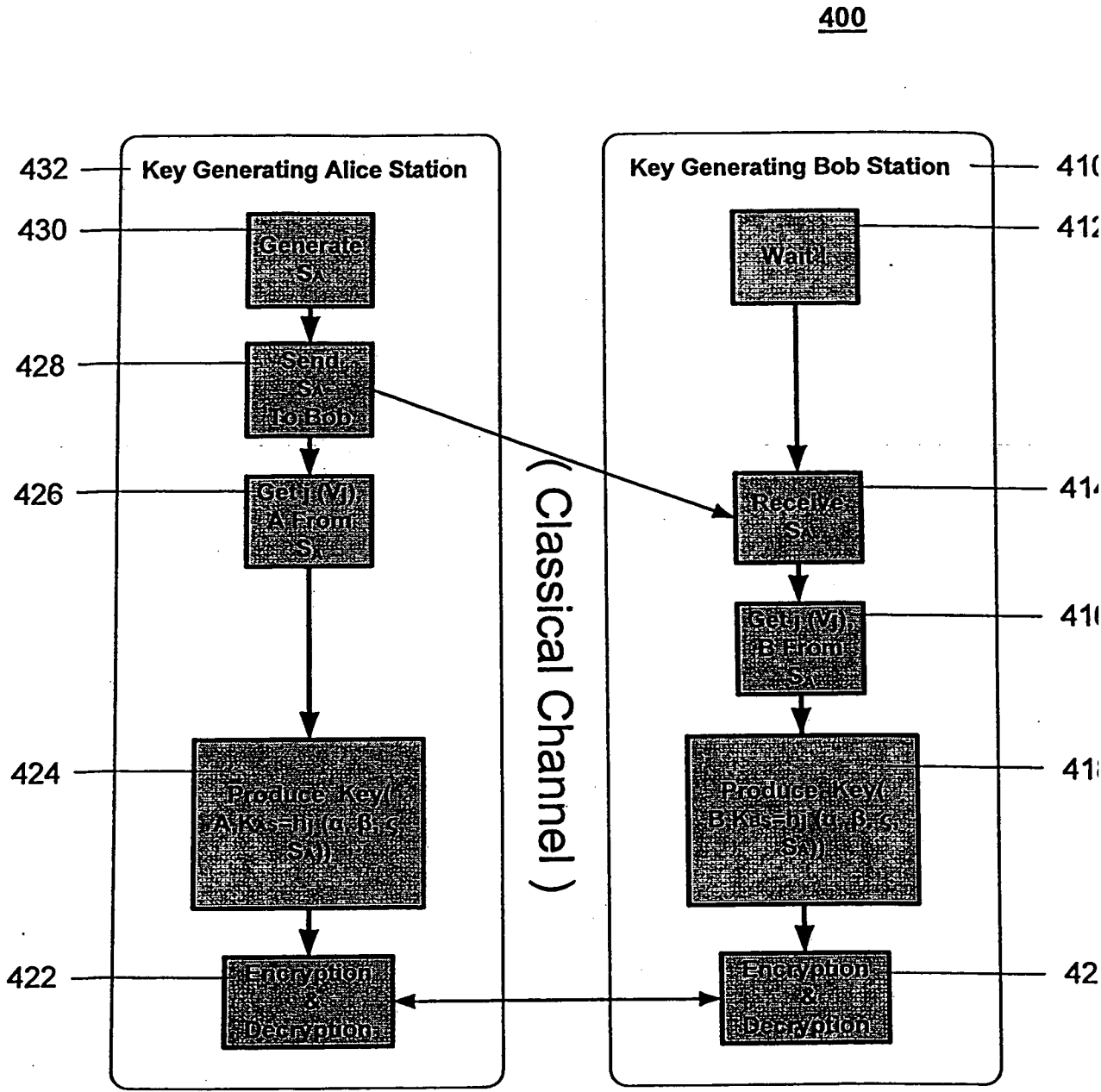


Fig. 4

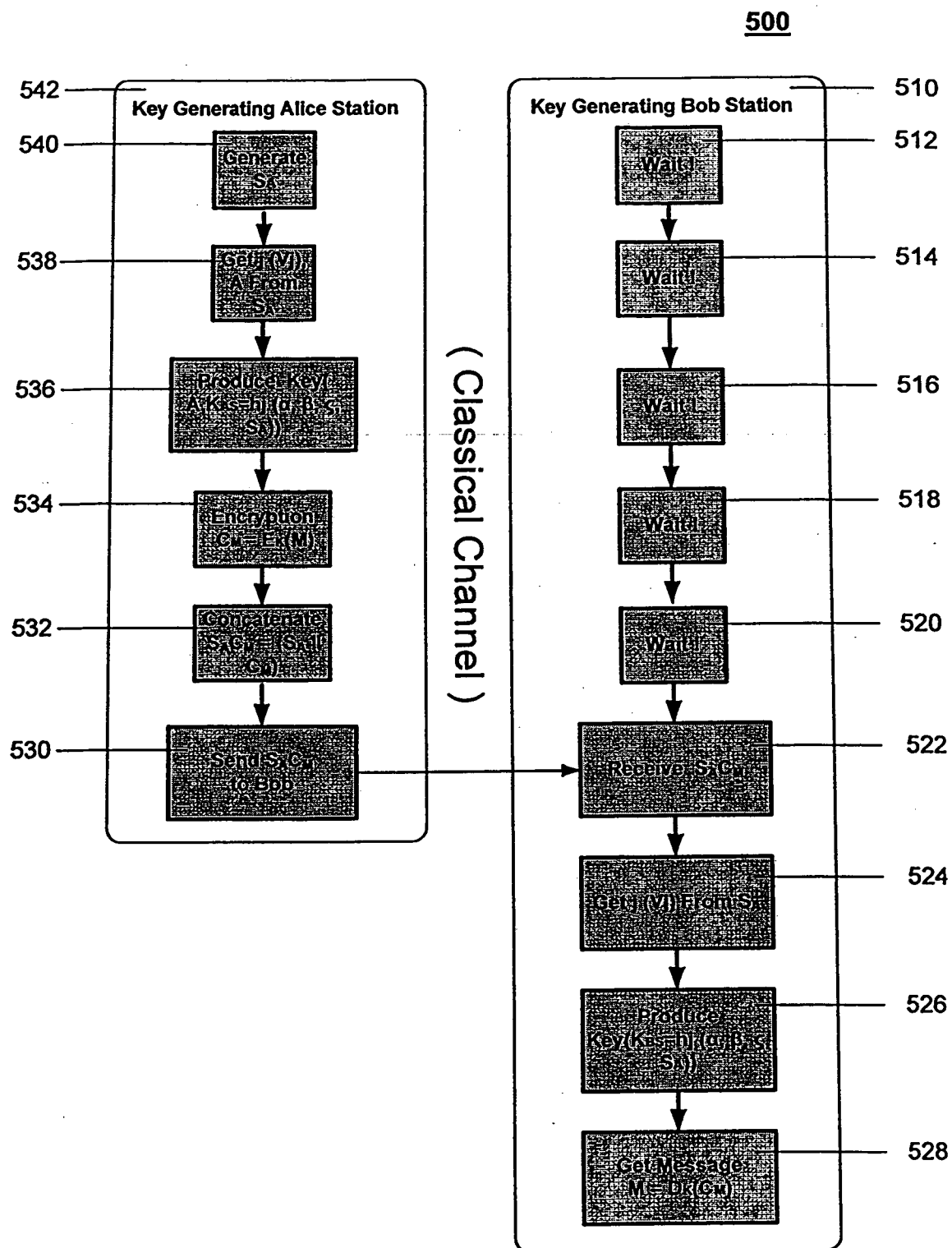


Fig. 5