



- (51) International Patent Classification:
H04L 9/20 (2006.01)
- (21) International Application Number:
PCT/MY2011/000248
- (22) International Filing Date:
27 December 2011 (27.12.2011)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
PI 2011000002 3 January 2011 (03.01.2011) 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): **SHARIPAH, Setapa** [MY/MY]; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **MOHD AMINUDIN MOHD, Khalid** [MY/MY]; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **NORAZAH, Abd Aziz** [MY/MY]; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **MOHD FAIZAL, Mubarak** [MY/MY]; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **JAMALUL-LAIL, Ab Manan** [MY/MY]; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **AZIMAH, Abdul**
- Kadir** [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, QA, RO, RS, RU, RW, 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, RW, 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, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: PSEUDONYM ID PRIVACY ENHANCEMENT

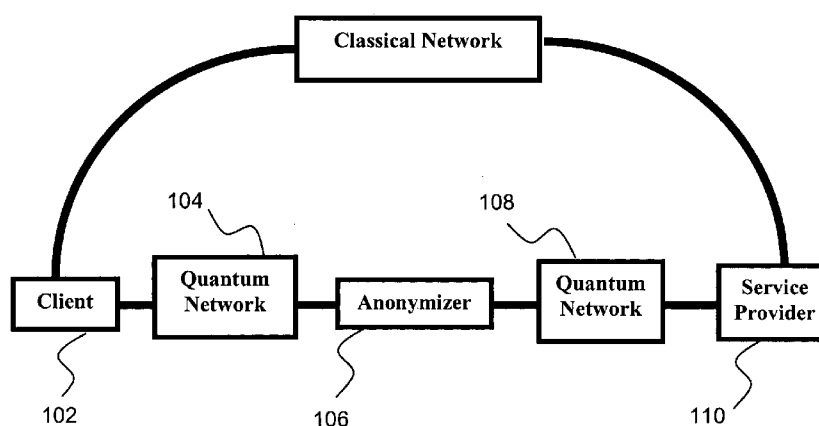


FIG. 1

(57) Abstract: The present invention provides system for solving predictability of pseudonym by using privacy enhancement mechanism and quantum key distribution. The system comprises at least one client application, at least one q-anonymizer, at least one quantum key distribution network between client application and q-anonymizer, at least one quantum key distribution network between q-anonymizer and service provider and a service provider. The at least one q-anonymizer validates independent communication between client application and q-anonymizer and further anonymize user identity between client application and service provider.



Declarations under Rule 4.17:

Published:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))* — *with international search report (Art. 21(3))*

PSEUDONYM ID PRIVACY ENHANCEMENT

FIELD OF INVENTION

5 The present invention relates to a system and method for solving predictability of pseudonym by using privacy enhancement mechanism and quantum key distribution (QKD).

BACKGROUND ART

10 Pseudonym identifier (ID) is used to protect user identity in ordinary privacy enhancement system wherein user is anonymous to e-Service Provider. The weakness of pseudonym ID is traceability of a user's identity to the pseudonym ID because methodology used to create pseudonym ID is structured and predictable. At present,
15 pseudonym ID is generated using hash function based on user's identity. A timestamp is used as input to hash function to change value of pseudonym ID for each communication session, which is less linkable to user's identity. The methodology of the timestamp is fixed, structured and predictable, which allows hacking by tracing the linkage. Thus, the entire system is thereby exposed to identity theft attack.

20 The present invention uses both privacy enhancement mechanisms and QKD to protect user privacy and to enhance system trust. The present invention introduces anonymizer in QKD network to provide privacy enhancement service and to reinforce unlinkability through randomness of q-anonymizer. The present invention provides the following
25 advantages:-

- a) QKD based privacy;
- b) strong privacy properties of QKD which enforces protection of personal data;
- c) identity is untraceable;
- d) identical key which provide authenticity between client and q-anonymizer, q-
30 anonymizer and service provider which protects network from phishing attack;
- e) trusted and auditable by q-anonymizer system.

The approach in the present invention provides solution towards predictability of pseudonym by using an alternative method provided by Quantum Key Distribution

(QKD) network. The characteristic and features of QKD enables incorporation of random process which complicates traceability of user identity. QKD network is unconditionally secure and private based on trusted QKD infrastructure as Q-anonymizer will be trusted anonymizer's engine.

5

Once secret key has been established by QKD, it can be used for variety of purposes. One of the purposes of the present invention is to use it as a seed to generate pseudonym ID by using anonymizer to produce quantum network based pseudonym ID. As QKD research continues, QKD devices will become more robust, easier to configure,
10 less expensive and smaller.

The subject matter claimed herein is not limited to embodiments that solve any disadvantages or that operate only in environments such as those described above. Rather, this background is only provided to illustrate one exemplary technology area
15 where some embodiments described herein may be practiced.

SUMMARY OF INVENTION

The present invention provides a system (100) for solving predictability of pseudonym by using privacy enhancement mechanism and quantum key distribution (QKD). The system comprising at least one client application (102), at least one q-anonymizer (106), at least one quantum key distribution (QKD) network between client application and q-anonymizer (104), at least one quantum key distribution (QKD) network between q-anonymizer and service provider (108) and a service provider (110). The at least one q-anonymizer (106) validates independent communication between client application and q-anonymizer and further anonymize user identity between client application and service provider.

Preferably, the at least one quantum key distribution (QKD) network between client application and q-anonymizer (104) generates shared secret key K_1 and identifier key (ID) while the at least one quantum key distribution (QKD) network between q-anonymizer and service provider (108) generates shared secret key K_2 and identifier key (ID).

Further, the said q-anonymizer (104) anonymize user identity between client application and service provider by generating quantum key distribution (QKD) based pseudonym identifier (ID) using at least XOR function in order to protect user identities during communication over QKD network. The said quantum key distribution network (QKD) based pseudonym identifier (ID) will expire based on quantum key which generates only one session.

Another aspect of the present invention provides a method for solving predictability of pseudonym by using privacy enhancement mechanism and quantum key distribution (QKD). The method comprising steps of initiating request to q-anonymizer (502), generating shared secret key K_1 and identifier key (ID) between client application and q-anonymizer via quantum key distribution (QKD) network (504), transmitting shared secret key K_1 and identifier key (ID) to client application and transmitting identifier key to q-anonymizer (506), retrieving shared secret key K_1 by q-anonymizer from quantum key distribution (QKD) network (508), establishing trusted communication between client application and q-anonymizer (514), generating shared secret key K_2 and identifier key

(ID) between q-anonymizer and service provider via quantum key distribution (QKD) network (602), retrieving shared secret key K_2 and identifier key (ID) from quantum key distribution (QKD) network and transmitting identifier key (ID) to service provider by q-anonymizer (604), transmitting shared secret key K_2 from quantum key distribution (QKD) network to service provider (606), establishing trusted communication between service provider and q-anonymizer by anonymizing user identity (612) and creating quantum key distribution (QKD) network based pseudonym identifier (ID) in q-anonymizer for privacy enhancement (700).

Preferably, the method for retrieving shared secret key K_1 by q-anonymizer from quantum key distribution (QKD) network further comprises performing challenge response to determine if communication is trusted (512) wherein communication between client application and q-anonymizer will be aborted (514) if challenge response fails; else trusted communication is established. Further, the method for retrieving shared secret key K_2 and identifier key (ID) from quantum key distribution (QKD) network and transmitting identifier key (ID) to service provider by q-anonymizer further comprises performing challenge response to determine if communication is trusted (608) wherein communication between client application and q-anonymizer will be aborted (610) if challenge response fails; else trusted communication is established.

Another aspect of the present invention provides a method (700) for creating quantum key distribution (QKD) network based pseudonym identifier (ID) in q-anonymizer for privacy enhancement. The method comprises retrieving shared secret keys K_1 and K_2 from quantum key distribution (QKD) network between client and service provider (702), generating final key by combining shared secret keys K_1 and K_2 using XOR function (704) and combining pseudonym identifier (ID) key with final key to produce quantum key distribution (QKD) network based pseudonym identifier (ID) (706).

The present invention consists of features and a combination of parts hereinafter fully described and illustrated in the accompanying drawings, it 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 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
5 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 illustrates a system (100) for solving predictability of pseudonym by using privacy enhancement mechanism and quantum key distribution (QKD).

FIG. 2 illustrates communications between Node 1 and Node 2 as well as between Node 2 and Node 3.

15 FIG. 3 illustrates trusted communication between client and q-anonymizer.

FIG. 4 illustrates q-anonymizer which anonymizes identity between client and service provider.

20 FIG. 5 is a flowchart illustrating methodology for establishing trusted communication between client and Q-anonymizer.

FIG. 6 is a flowchart illustrating methodology for establishing trusted communication between service provider and q-anonymizer by anonymizing user identity.

25 FIG. 7 is a flowchart illustrating methodology for creating quantum key distribution (QKD) network based pseudonym identifier (ID) in q-anonymizer for privacy enhancement.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention provides a system and method for solving predictability of pseudonym by using privacy enhancement mechanism and quantum key distribution (QKD). Hereinafter, this specification will describe the present invention according to the preferred embodiments. 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 without departing from the scope of the appended claims.

Reference is first made to FIG. 1. FIG. 1 illustrates a system (100) for solving predictability of pseudonym by using privacy enhancement mechanism and quantum key distribution (QKD). As illustrated in FIG. 1, the system comprising at least one client application (102), at least one q-anonymizer (106), at least one quantum key distribution (QKD) network between client application and q-anonymizer (104), at least one quantum key distribution (QKD) network between q-anonymizer and service provider (108) and a service provider (110).

QKD box of quantum network (102, 108) generates shared keys K_1 and K_2 and identifier (ID) key wherein the at least one quantum key distribution (QKD) network between client application and q-anonymizer (104) generates shared secret key K_1 and identifier key (ID). The at least one quantum key distribution (QKD) network between q-anonymizer and service provider (108) generates shared secret key K_2 and identifier key (ID).

The at least one q-anonymizer (106) validates independent communication between client application and q-anonymizer and further anonymize user identity between client application and service provider. The said q-anonymizer (104) anonymize user identity between client application and service provider by generating quantum key distribution (QKD) based pseudonym identifier (ID) using at least XOR function in order to protect user identities during communication over QKD network.

Reference is now being made to FIG. 2. FIG. 2 illustrates communications between Node 1 and Node 2 as well as between Node 2 and Node 3. As illustrated in FIG. 2, client in node 1 receives shared key K_1 from QKD system and transmits key to q-anonymizer. The shared key K_1 and ID key are generated through quantum link. Both identical keys, K_1 and K_2 , are stored in database together with ID key in node 1 and 2.

Upon receiving ID key, q-anonymizer retrieves shared key K_1 through link 1 in node 2. Communication is established between client and q-anonymizer. In node 2, q-anonymizer retrieves shared key K_2 from QKD system wherein shared key K_2 and ID key is generated through link 2. Service provider in node 3 receives ID key from q-anonymizer. Service provider retrieves shared key K_2 from QKD system through link 2 using key ID which establishes communication between Q-anonymizer and service provider. Thereafter, K_2 is combined with pseudonym ID in order to obtain quantum-based pseudonym ID.

Reference is now being made to FIG. 3. FIG. 3 illustrates trusted communication between client and q-anonymizer. As illustrated in FIG. 3, client application receives shared key K_1 from QKD system. The key ID is sent to q-anonymizer wherein q-anonymizer retrieves key K_1 from QKD system which establishes communication between client and q-anonymizer. In node 2, q-anonymizer retrieves key K_2 from QKD system using link 2. Service provider receives key ID from Q-anonymizer. Using key ID, service provider receives shared key K_2 from QKD system which establishes communication between service provider and Q-anonymizer in node 2.

Reference is now being made to FIG. 4. FIG. 4 illustrates q-anonymizer which anonymizes identity between client and service provider. As illustrated in FIG. 4, shared key K_1 will be combined with shared key K_2 using XOR function in q-anonymizer which results in the final key. Pseudonym ID will then be combined with final key to obtain QNet-based pseudonym ID which protects user personnel identity for privacy.

Reference is now being made to FIG. 5 and FIG. 6 respectively. FIG. 5 is a flowchart illustrating methodology for establishing trusted communication between client and Q-anonymizer while FIG. 6 is a flowchart illustrating methodology for establishing trusted communication between service provider and q-anonymizer by anonymizing user identity. As illustrated in FIG. 5, a method for solving predictability of pseudonym by using privacy enhancement mechanism and quantum key distribution (QKD) comprising steps of initiating request to q-anonymizer (502) and generating shared secret key K_1 and identifier key (ID) between client application and q-anonymizer via quantum key distribution (QKD) network (504). Thereafter, shared secret key K_1 and identifier key (ID) is transmitted to client application and further transmitting identifier key to q-anonymizer

(506). Shared secret key K_1 is retrieved by q-anonymizer from quantum key distribution (QKD) network (508). Further, challenge response is performed to determine if communication is trusted (512) wherein communication between client application and q-anonymizer will be aborted (514) if challenge response fails; else trusted communication is established. Trusted communication is established between client application and q-anonymizer if challenge response is successful (512).

As illustrated in FIG. 6, shared secret key K_2 and identifier key (ID) is generated between q-anonymizer and service provider via quantum key distribution (QKD) network (602). Thereafter, shared secret key K_2 and identifier key (ID) is retrieved from quantum key distribution (QKD) network (604). Further, q-anonymizer transmits identifier key (ID) to service provider (604). Challenge response is performed to determine if communication is trusted (608) wherein communication between client application and q-anonymizer will be aborted (610) if challenge response fails; else trusted communication is established.

Shared secret key K_2 is transmitted from quantum key distribution (QKD) network to service provider (606) which establishes trusted communication between service provider and q-anonymizer by anonymizing user identity (612). Quantum key distribution (QKD) network based pseudonym identifier (ID) is thereafter created in q-anonymizer for privacy enhancement (700).

Reference is now being made to FIG. 7. FIG. 7 is a flowchart illustrating methodology for creating quantum key distribution (QKD) network based pseudonym identifier (ID) in q-anonymizer for privacy enhancement. As illustrated in FIG. 7, quantum key distribution (QKD) network based pseudonym identifier (ID) is created in q-anonymizer for privacy enhancement by retrieving shared secret keys K_1 and K_2 from quantum key distribution (QKD) network between client and service provider (702). Thereafter, final key is generated by combining shared secret keys K_1 and K_2 using XOR function (704) and combining pseudonym identifier (ID) key with final key to produce quantum key distribution (QKD) network based pseudonym identifier (ID) (706).

Shared secret key K_1 and shared secret key K_2 are randomly generated via quantum key distribution (QKD) network to enhance unlinkability between client and service provider. Quantum key distribution network (QKD) based pseudonym identifier (ID) of the present

invention will expire based on quantum key which generates only one session. User's identity is anonymous as pseudonym ID is combined with quantum key which allows for double layer to increase unlinkability, privacy. Q-anonymizer is trusted and is part of QKD network that is secure and private. Thus, the present invention prevents QKD
5 network based pseudonym ID from being traced back to the user as only q-anonymizer will know the user identity.

The approach in the present invention provides solution towards predictability of pseudonym by using an alternative method provided by Quantum Key Distribution
10 (QKD) network. The characteristic and features of QKD enables incorporation of random process which complicates traceability of user identity. QKD network is unconditionally secure and private based on trusted QKD infrastructure as Q-anonymizer will be trusted anonymizer's engine.

15 The present invention may be embodied in other specific forms without departing from its essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore indicated by the appended claims rather than by the foregoing description. All changes, which come within the meaning and range of equivalency of the claims, are to be
20 embraced within their scope.

CLAIMS

1. A system (100) for solving predictability of pseudonym by using privacy enhancement mechanism and quantum key distribution (QKD) comprising:
 - 5 at least one client application (102);
 - at least one q-anonymizer (106);
 - at least one QKD network between client application and q-anonymizer (104);
 - at least one QKD network between q-anonymizer and service provider (108); and
 - 10 a service provider (110);
 - characterized in that the at least one q-anonymizer (106) validates independent communication between client application and q-anonymizer and further anonymize user identity between client
 - 15 application and service provider.
2. A system according to Claim 1 wherein the at least one quantum key distribution (QKD) network between client application and q-anonymizer (104) generates shared secret key K_1 and identifier key (ID).
- 20 3. A system according to Claim 1, wherein the at least one QKD network between q-anonymizer and service provider (108) generates shared secret key K_2 and identifier key (ID).
- 25 4. A system according to Claim 1, wherein the said q-anonymizer (104) anonymize user identity between client application and service provider by generating QKD based pseudonym ID using at least XOR function in order to protect user identities during communication over QKD network.
- 30 5. A system according to Claim 1 and Claim 4, wherein the said QKD based pseudonym ID will expire based on quantum key which generates only one session.

6. A method for solving predictability of pseudonym by using privacy enhancement mechanism and quantum key distribution (QKD) comprising steps of:

initiating request to q-anonymizer (502);

generating shared secret key K_1 and ID key between client application and q-anonymizer via QKD network (504);

transmitting shared secret key K_1 and ID key to client application and transmitting ID key to q-anonymizer (506);

retrieving shared secret key K_1 by q-anonymizer from QKD network (508);

establishing trusted communication between client application and q-anonymizer (514);

generating shared secret key K_2 and ID key between q-anonymizer and service provider via QKD network (602);

retrieving shared secret key K_2 and ID key from QKD network and transmitting ID key to service provider by q-anonymizer (604);

transmitting shared secret key K_2 from QKD network to service provider (606);

establishing trusted communication between service provider and q-anonymizer by anonymizing user identity (612); and

creating QKD network based pseudonym identifier (ID) in q-anonymizer for privacy enhancement (700).

7. A method according to Claim 6 wherein retrieving shared secret key K_1 by q-anonymizer from QKD network further comprises performing challenge response to determine if communication is trusted (510) wherein communication between client application and q-anonymizer will be aborted (512) if challenge response fails; else trusted communication is established.

8. A method according to Claim 6 wherein retrieving shared secret key K_2 and ID key from QKD network and transmitting ID key to service provider by q-anonymizer further comprises performing challenge response to determine if communication is trusted (608) wherein communication between client application and q-anonymizer will be aborted (610) if challenge response fails; else trusted communication is established.

9. A method (700) according to Claim 6 wherein creating QKD network based pseudonym ID in q-anonymizer for privacy enhancement further comprises:
- retrieving shared secret keys K_1 and K_2 from QKD network between client and service provider (702);
- 5 generating final key by combining shared secret keys K_1 and K_2 using XOR function (704); and
- combining pseudonym ID key with final key to produce QKD network based pseudonym ID (706).
- 10 10. A method according to Claim 6 wherein shared secret key K_1 and shared secret key K_2 are randomly generated via QKD network to enhance unlinkability between client and service provider.

100

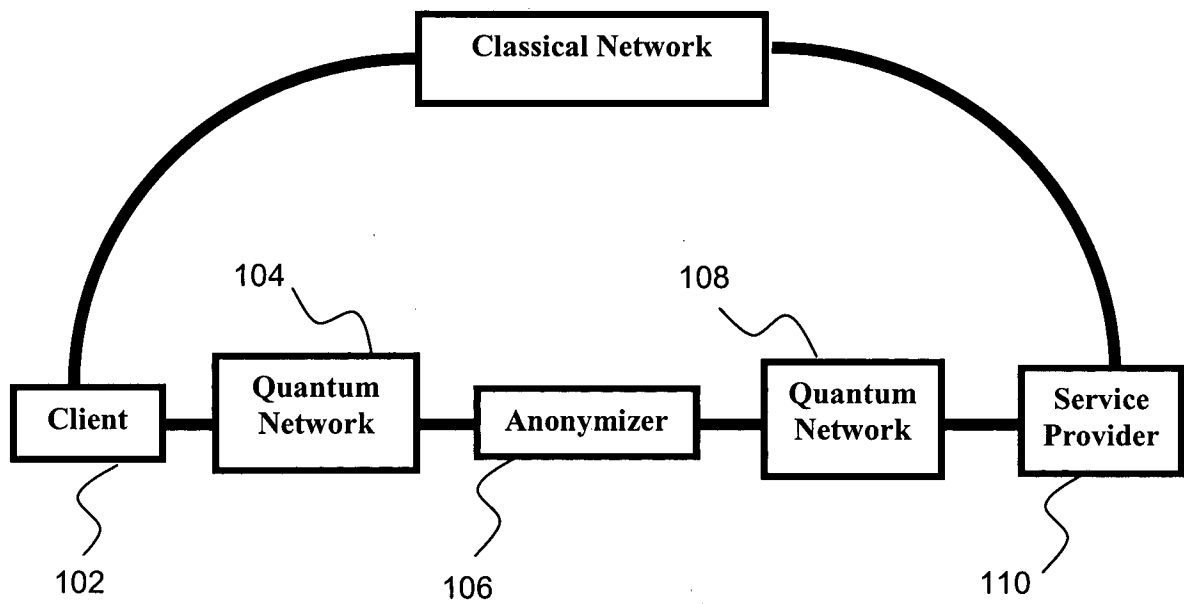


FIG. 1

200

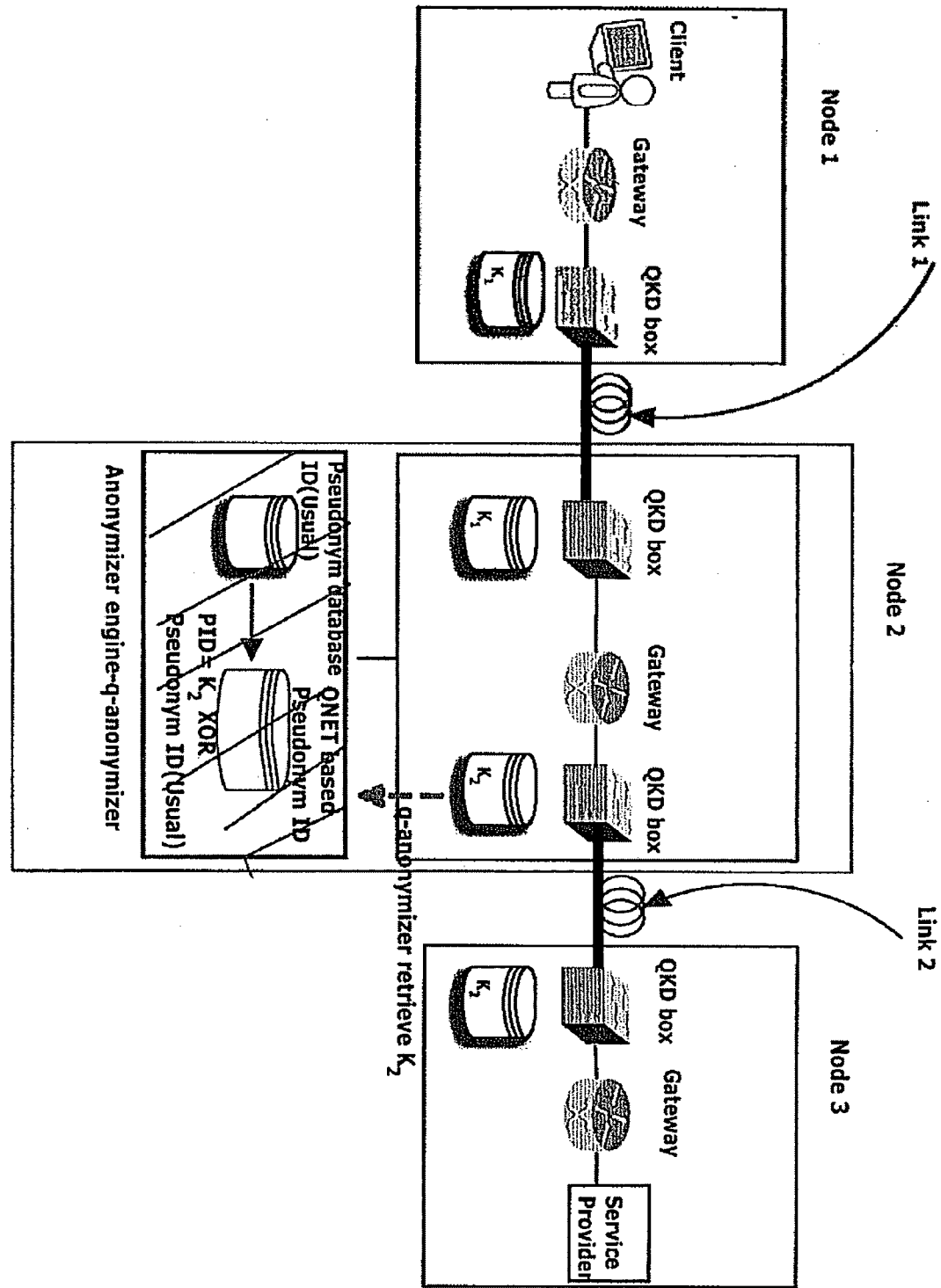


FIG. 2

300

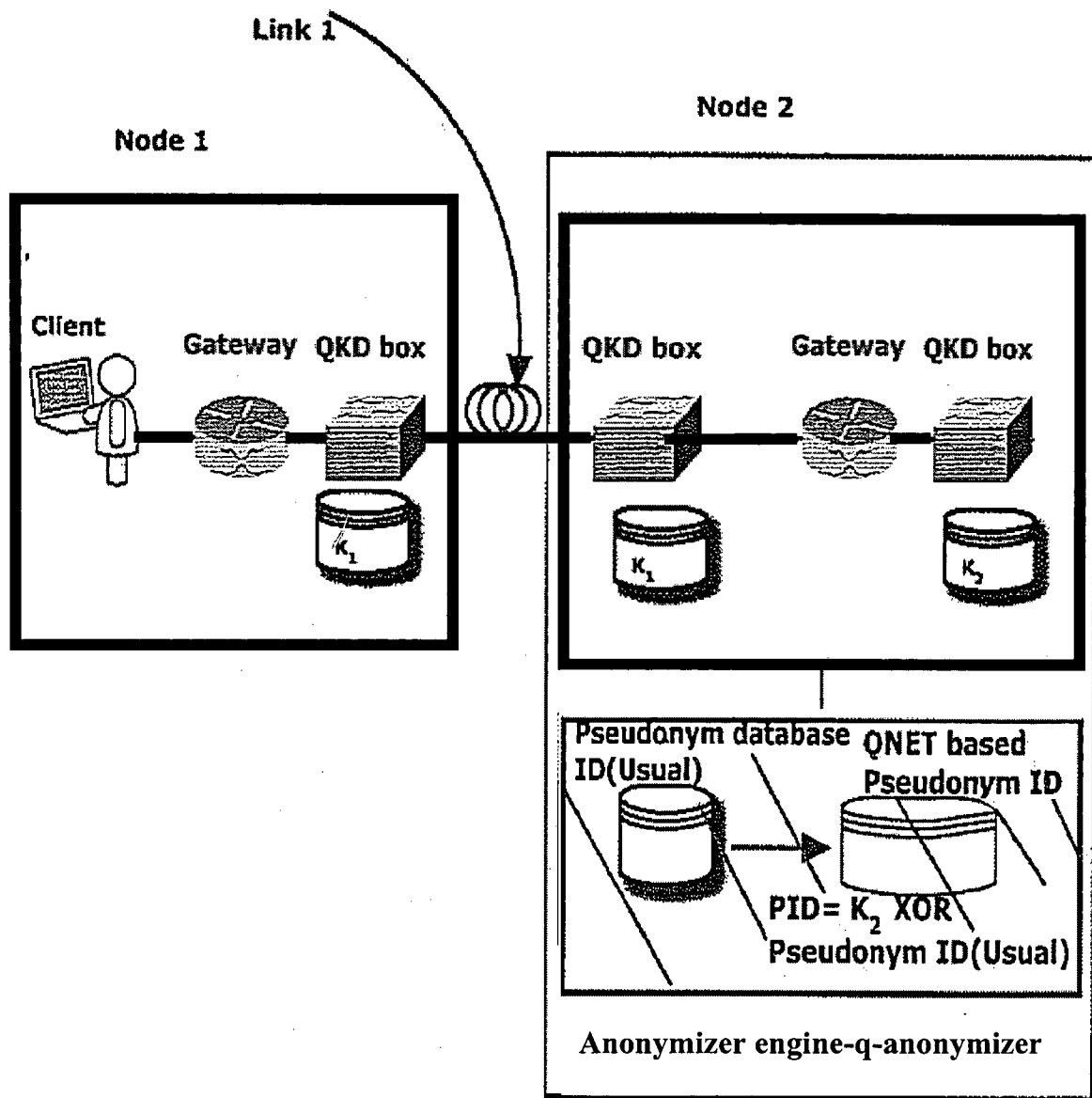


FIG. 3

400

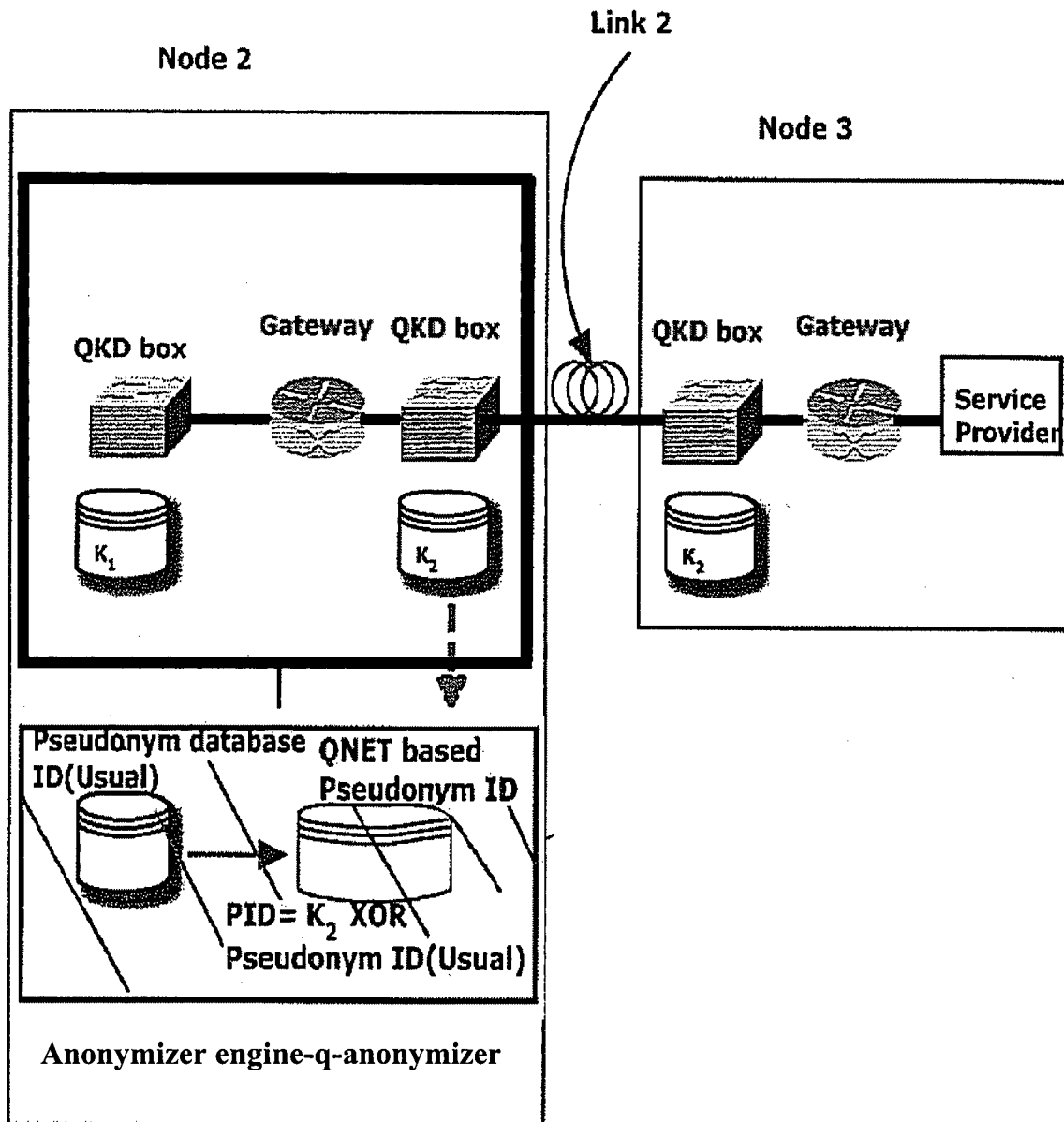


FIG. 4

5/7

500

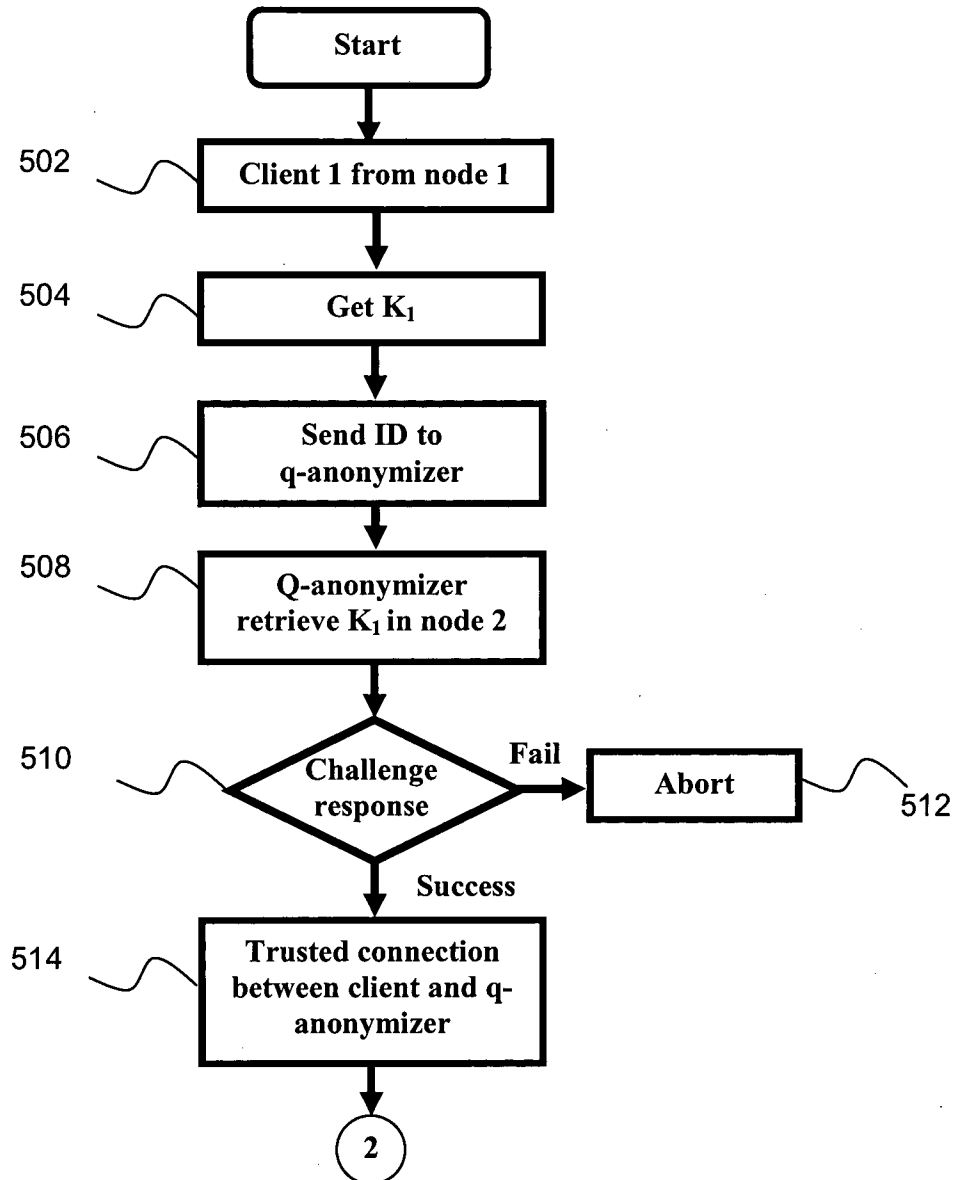


FIG. 5

600

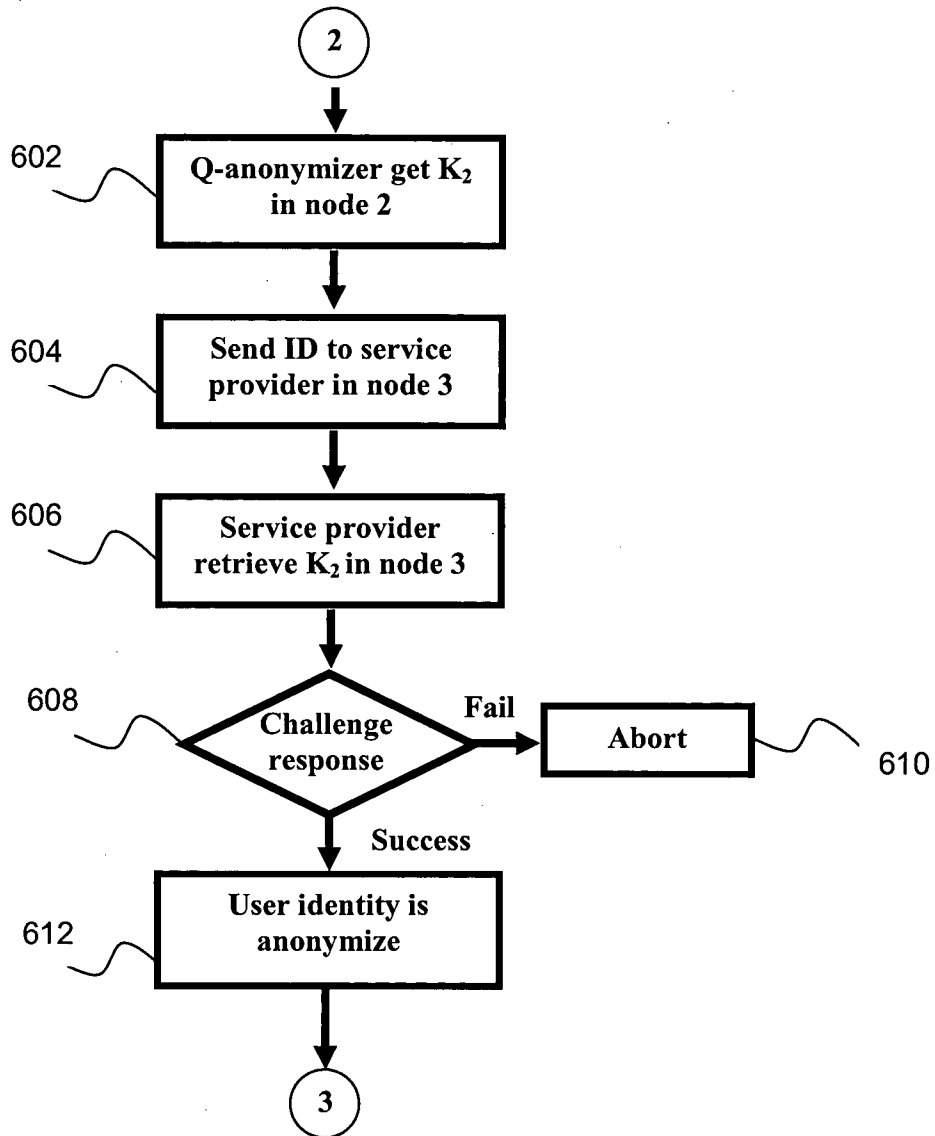


FIG. 6

7/7

700

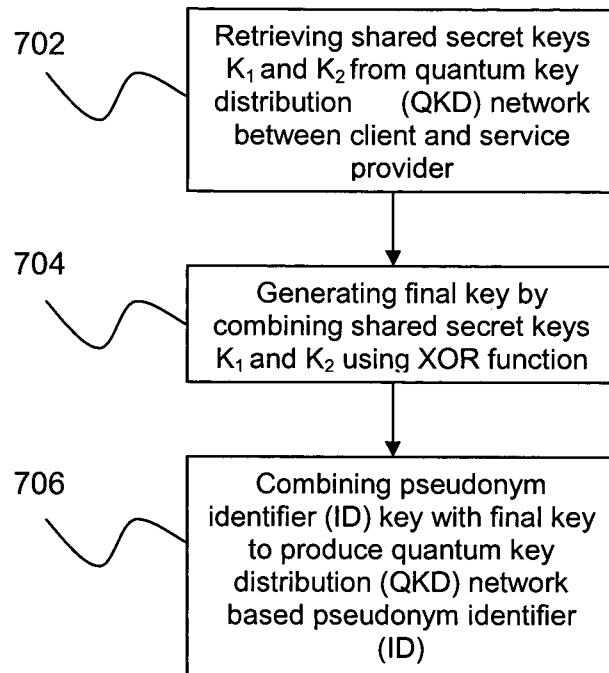


FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/MY2011/000248

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.

H04L 9/20 (2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

DWPI & EPODOC - Keywords (pseudonym, privacy, QKD, anonymizer, validate) and like terms; Google Patent search – keywords (qkd, anonymizer, pseudonym)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P, X	Pseudonym and Privacy Using Quantum Key Distribution (QKD) in E-business - IJCSNS International Journal of Computer Science and Network Security, Vol.11 No. 8, August 2011 (SETAPA et al) – retrieved from http://paper.ijcsns.org/07_book/201108/20110822.pdf on 21 February 2012 Pages 151-154	1-10
A	US 2009/0041239 A1 (TERANISHI) 12 February 2009 Abstract	
A	US 7234059 B1 (BEAVER et al) 19 June 2007 Abstract	



Further documents are listed in the continuation of Box C



See patent family annex

* Special categories of cited documents:	
"A" document defining the general state of the art which is not considered to be of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"E" earlier application or patent but published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search

24 February 2012

Date of mailing of the international search report

8 March 2012

Name and mailing address of the ISA/AU

AUSTRALIAN PATENT OFFICE
PO BOX 200, WODEN ACT 2606, AUSTRALIA
E-mail address: pct@ipaustalia.gov.au
Facsimile No. +61 2 6283 7999

Authorized officer

JAE CHO
AUSTRALIAN PATENT OFFICE
(ISO 9001 Quality Certified Service)
Telephone No : +61 2 6222 3668

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/MY2011/000248

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member	
US	2009041239	CA 2609166 WO 2006126668	EP 1898382 JP 2006330462
US	7234059	NONE	
Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.			
END OF ANNEX			