

CLAIMS:

1. A computer-implemented method of determining, at a first node (C), a common secret (CS) that is common with the first node (C) and a second node (S), wherein the first node (C) is associated with a first asymmetric cryptography pair of a cryptography system having a homomorphic property, the first asymmetric cryptography pair having a first node master private key (V_{1C}) and a first node master public key (P_{1C}), and the second node (S) is associated with a second asymmetric cryptography pair of the cryptography system, the second asymmetric cryptography pair having a second node master private key (V_{1S}) and a second node master public key (P_{1S}), wherein the first node master public key and second node master public key are based on encryption of respective first node master private key and second node master private key using the cryptography system common with the first and second nodes, and wherein the method comprises:

- determining a first node second private key (V_{2C}) based on at least the first node master private key (V_{1C}) and a deterministic key (DK) common with the first and second nodes;

- determining a second node second public key (P_{2S}) based on at least the second node master public key (P_{1S}) and encryption of the deterministic key (DK) using the common cryptography system; and

- determining the common secret (CS) based on encryption of the first node second private key (V_{2C}), using the common cryptography system, and the second node second public key (P_{2S}),

wherein the second node (S) has the same common secret (S) based on a first node second public key (P_{2C}) and encryption of a second node second private key (V_{2S}) using the common cryptography system, wherein:

- the first node second public key (P_{2C}) is based on at least the first node master public key (P_{1C}) and encryption of the deterministic key (DK) using the common cryptography system; and

- the second node second private key (V_{2S}) is based on at least the second node master private key (V_{1S}) and the deterministic key (DK).

2. A method according to claim 1, including one or more of the following features:

(i) wherein the deterministic key (DK) is based on a message (M);

(ii) wherein the cryptography system is an elliptic curve cryptography (ECC) system and the first node master public key (P_{1C}) and second node master public key (P_{1S}) are based on elliptic curve point multiplication of respective first node master private key (V_{1C}) and second node master private key (V_{1S}) and a generator (G);

(iii) further comprising the steps of:

- receiving, over the communications network, the second node master public key (P_{1S}); and

- storing, at a data store associated with the first node (C), the second node master public key (P_{1S});

(iv) further comprising the steps of:

- generating, at a first node (C), the first node master private key (V_{1C}) and the first node master public key (P_{1C});

- sending, over the communications network, the first node master public key (P_{1C}) to the second node (S) and/or other node; and

- storing, in a first data store associated with the first node (C), the first node master private key (V_{1C});

(v) wherein the deterministic key (DK) is based on determining a hash of a previous deterministic key; or

(vi) wherein the first asymmetric cryptography pair and the second asymmetric cryptography pair are based on a function of respective previous first asymmetric cryptography pair and previous second asymmetric cryptography pair.

3. A method according to claim 2 including one or more of the following features:

(i) further comprising:

- generating a first signed message (SM1) based on the message (M) and the first node second private key (V_{2C}); and

- sending, over the communications network, the first signed message (SM1) to the second node (S),

wherein the first signed message (SM1) can be validated with a first node second public key (P_{2C}) to authenticate the first node (C);

(ii) further comprising:

- receiving, over the communications network, a second signed message (SM2) from the second node (S);

- validating the second signed message (SM2) with the second node second public key (P_{2S}); and

- authenticating the second node (S) based on the result of validating the second signed message (SM2),

wherein the second signed message (SM2) was generated based on the message (M), or a second message (M2), and the second node second private key (V_{2S});

(iii) further comprising:

- generating a message (M); and

- sending, over a communications network, the message (M) to the second node (S);

(iv) further comprising:

- receiving the message (M), over the communications network, from the second node (S);

(v) further comprising:

- receiving the message (M), over the communications network, from another node;

(vi) further comprising:

- receiving the message (M) from a data store, and/or an input interface associated with the first node (C); or

(vii) further comprising:

- sending, over the communications network, to the second node, a notice indicative of using a common cryptography system for the method of determining a common secret (CS), and

wherein the step of generating the first node master private key (V_{1C}) and the first node master public key (P_{1C}) comprises:

- generating the first node master private key (V_{1C}) based on a random integer in an allowable range specified in the common cryptography system; and

- determining the first node master public key (P_{1C}) based on encryption of the first node master private key (V_{1C}) .

4. A method according to claim 3, wherein the common cryptography system is an elliptic curve cryptography (ECC) system with a common generator (G) and the first node master public key (P_{1C}) is determined based on elliptic curve point multiplication of the first node master private key (V_{1C}) and the common generator (G) according to the following formula:

$$P_{1C} = V_{1C} \times G.$$

5. A method according to claim 4 further comprising:

- determining the deterministic key (DK) based on determining a hash of the message (M), and

wherein the step of determining a first node second private key (V_{2C}) is based on a scalar addition of the first node master private key (V_{1C}) and the deterministic key (DK) according to the following formula:

$$V_{2C} = V_{1C} + DK, \text{ and}$$

wherein the step of determining a second node second public key (P_{2S}) is based on the second node master public key (P_{1S}) with elliptic curve point addition to the elliptic curve point multiplication of the deterministic key (DK) and the common generator (G) according to the following formula:

$$P_{2S} = P_{1S} + DK \times G.$$

6. A method of secure communication between a first node and a second node with symmetric-key algorithm, wherein the method comprises:

determining a common secret by means of a method according to any one of the preceding claims;

- determining a symmetric-key based on the common secret;

- encrypting a first communication message, with the symmetric-key, to an encrypted first communication message; and

- sending, over a communications network, the encrypted first communication message from the first node (C) to the second node (S).

7. The method according to claim 6, wherein the method further comprises:

- receiving, over a communications network, an encrypted second communication message from the second node (S); and

- decrypting the encrypted second communication message, with the symmetric-key, to a second communication message.

8. A method of performing an online transaction between a first node and a second node, wherein the method comprises:

determining a common secret by means of a method according to any one of claims 1 to 5;

- determining a symmetric-key based on the common secret;

- encrypting a first transaction message, with the symmetric-key, to an encrypted first transaction message;

- sending, over a communications network, the encrypted first transaction message from the first node (C) to the second node (S);

- receiving, over a communications network, an encrypted second transaction message from the second node (S); and

- decrypting the encrypted second transaction message, with the symmetric-key, to a second transaction message.

9. A device for determining, at a first node (c), a common secret (CS) that is common with a second node (S), wherein the first node (C) is associated with a first asymmetric cryptography pair having a first node master private key (V_{1C}) and a first node master public key (P_{1C}), and the second node (S) is associated with a second asymmetric cryptography pair having a second node master private key (V_{1S}) and a second node master public key (P_{1S}), wherein the device comprises a first processing device to perform the method according to any one of the preceding claims to determine the common secret.

10. A device for secure communication, or performing a secure online transaction between a first node and a second node, wherein the device includes a first processing device to:

- perform the method according to any one of claims 6 to 8.

11. A device according to claim 9 or 10, including one or more of the following features:

- (i) further comprising a first data store to store one or more of the first node master private key (V_{1C}); or

- (ii) further comprising a communications module to send and/or receive, over a communications network, one or more of the message (M), the first node master public key (P_{1C}), the second node master public key (P_{1S}), the first signed message (SM1), the second signed message (SM2), the notice indicative of using a common cryptography system.

12. A device according to claim 11, including one or more of the following features:

- (i) wherein the first data store further stores one or more of the first node master public key (P_{1C}), the second node master public key (P_{1S}), and the message (M); or

- (ii) wherein the common cryptography system is an elliptic curve cryptography (ECC) system with a common generator (G).

13. A system for determining a common secret between a first node (C) and a second node (S), wherein:

- the first node (C) is associated with a first asymmetric cryptography pair of a cryptography system having a homomorphic property, the first asymmetric cryptography pair having a first node master private key (V_{1C}) and a first node master public key (P_{1C}); and

- the second node (S) is associated with a second asymmetric cryptography pair of the cryptography system, the second asymmetric cryptography pair having a second node master private key (V_{1S}) and a second node master public key (P_{1S}), wherein the first node master public key and second node master public key are based on encryption of respective

first node master private key and second node master private key using the cryptography system common with the first and second nodes, and the system comprising:

- a first processing device, associated with the first node (C), configured to:
 - determine a first node second private key (V_{2C}) based on at least the first node master private key (V_{1C}) and a deterministic key (DK) common with the first and second nodes;
 - determine a second node second public key (P_{2S}) based on at least the second node master public key (P_{1S}) and encryption of the deterministic key (DK) using the common cryptography system; and
 - determine the common secret (CS) based on encryption of the first node second private key (V_{2C}), using the common cryptography system, and the second node second public key (P_{2S}); and
- a second processing device, associated with the second node (S), configured to:
 - determine a first node second public key (P_{2C}) based on at least the first node master public key (P_{1C}) and encryption of the the deterministic key (DK) using the common cryptography system; and
 - determine a second node second private key (V_{2S}) based on at least the second node master private key (V_{1S}) and the deterministic key (DK); and
 - determine the common secret based on the first node second public key (P_{2C}) and encryption of a second node second private key (V_{2S}) using the common cryptography system,

wherein the first processing device and the second processing device determine the same common secret.

14. A system according to claim 13, including one or more of the following features:

(i) wherein the deterministic key (DK) is based on a message (M), and the first processing device is further configured to:

- generate a first signed message (SM1) based on the message (M) and the first node second private key (V_{2C}); and

- send, over the communications network, the first signed message (SM1) to the second node (S),

wherein the second processing device is further configured to:

- receive the first signed message (SM1);

- validate the first signed message (SM1) with the first node second public key (P_{2C}); and

- authenticate the first node (C) based on a result of the validated first signed message (SM1);

(ii) wherein the second processing device is further configured to:

- generate a second signed message (SM2) based on the message (M), or a second message (M2), and the second node second private key (V_{2S}); and

- send the second signed message (SM2) to the first node (C),

wherein the first processing device is further configured to:

- receive the second signed message (SM2);

- validate the second signed message (SM2) with the second node second public key (P_{2S}); and

- authenticate the second node (S) based on a result of the validated second signed message (SM2);

(iii) wherein the first processing device is configured to:

- generate the message (M); and
- send the message (M),

wherein the second processing device is configured to:

- receive the message (M);

(iv) wherein the message is generated by another node, wherein the first processing device is configured to:

- receive the message (M),

wherein the second processing device is configured to:

- receive the message (M);

(v) further comprising a system data store and/or input interface, wherein the first processing device and second processing device receives the message (M), or the second message (M2) from the system data store and/or input interface;

(vi) wherein the cryptography system is an elliptic curve cryptography (ECC) system and the first node master public key (P_{1C}), second node master public key (P_{1S}) are based on elliptic curve point multiplication of respective first node master private key (V_{1C}) and second node master private key (V_{1S}) and a generator (G);

(vii) further comprising:

- a first data store associated with the first node (C) to store the first node master private key (V_{1C}); and

- a second data store associated with the second node (S) to store the second node master private key (V_{1S});

(viii) wherein the first processing device is further configured to:

- generate the first node master private key (V_{1C}) based on a random integer in an allowable range specified in a common cryptography system; and

- determine the first node master public key (P_{1C}) based on encryption of the first node master private key (V_{1C})

and wherein the second processing device is further configured to:

- generate the second node master private key (V_{1S}) based on a random integer in the allowable range specified in the common cryptography system; and

- determine the second node master public key (P_{1S}) based on encryption of the second node master private key (V_{1S});

(ix) wherein the first processing device is configured to:

- determine the deterministic key (DK) based on a hash of the message (M), and wherein:

- the first node second private key (V_{2C}) is based on a scalar addition of the first node master private key (V_{1C}) and the deterministic key (DK) according to the formula:

$$V_{2C} = V_{1C} + DK ; \text{ and}$$

- the second node public key (P_{2S}) is based on the second node master public key (P_{1S}) with elliptic curve point addition to the elliptic curve point multiplication of the deterministic key (DK) and the common generator (G) according to the following formula:

$$P_{2S} = P_{1S} + DK \times G$$

and wherein the second processing device is configured to:

- determine the deterministic key (DK) based on a hash of the message (M), and wherein:

- the second node second private key (V_{2S}) is based on a scalar addition of the second node master private key (V_{1S}) and the deterministic key (DK) according to the formula:

$$V_{2S} = V_{1C} + DK ; \text{ and}$$

- the first node public key (P_{2C}) is based on the first node master public key (P_{1C}) with elliptic curve point addition to the elliptic curve point multiplication of the deterministic key (DK) and the common generator (G) according to the following formula:

$$P_{2C} = P_{1C} + DK \times G;$$

(x) further comprising:

- a first communications module associated with the first processing device to send and/or receive, over a communications network, one or more of the message (M), the first node master public key (P_{1C}), the second node master public key (P_{1S}), the first signed message (SM1), the second signed message (SM2), and a notice indicative of using a common cryptography system; and

- a second communications module associated with the second processing device to send and/or receive, over a communications network, one or more of the message (M), the first node master public key (P_{1C}), the second node master public key (P_{1S}), the first signed message (SM1), the second signed message (SM2), and the notice indicative of using a common cryptography system;

(xi) wherein the deterministic key (DK) is based on determining a hash of a previous deterministic key; or

(xii) wherein the first asymmetric cryptography pair and the second asymmetric cryptography pair are based on a function of respective previous first asymmetric cryptography pair and previous second asymmetric cryptography pair.

15. A system according to claim 14, including one or more of the following features:

(i) wherein the first processing device receives the second node master public key (P_{1S}) from the system data store and/or input device, and the second processing device receives the first node master public key (P_{1C}) from the system data store and/or input device;

(ii) wherein the first processing device is configured to:

- generate the first node master private key (V_{1C}) and the first node master public key (P_{1C});

- send the first node master public key (P_{1C}); and

- store the first node master private key (V_{1C}) in the first data store,

wherein the second processing device is configured to:

- generate the second node master private key (V_{1S}) and the second node master public key (P_{1S});

- send the second node master public key (P_{1S}); and

- store the second node master private key (V_{1S}) in the second data store;

(iii) wherein:

- the first data store receives and stores the second node master public key (P_{1S}); and

- the second data store receives and stores the first node master public key (P_{1C});

(iv) wherein the common cryptography system is an elliptic curve cryptography (ECC) system with a common generator (G), wherein the first processing device is further configured to:

- determine the first node master public key (P_{1C}) based on elliptic curve point multiplication of the first node master private key (V_{1C}) and the common generator according to the formula:

$$P_{1C} = V_{1C} \times G.$$

and wherein the second processing device is further configured to:

- determine the second node master public key (P_{1S}) based on elliptic curve point multiplication of the second node master private key (V_{1S}) and the common generator according to the formula:

$$P_{1S} = V_{1S} \times G; \text{ or}$$

(v) wherein the common cryptography system is an elliptic curve cryptography (ECC) system with a common generator (G).

16. A system for secure communication between a first node and a second node with symmetric-key algorithm, wherein the system comprises:

- a system according to any one of claims 13 to 15 to determine a common secret with the first processing device and the second processing device, wherein the first processing device is further configured to:

- determine a symmetric-key based on the common secret;
- encrypt a first communication message, with the symmetric-key, to an encrypted first communication message; and
- send the encrypted first communication message;

wherein the second processing device is further configured to:

- determine the same symmetric-key based on the common secret;

- receive the encrypted first communication message; and

- decrypt the encrypted first communication message, with the symmetric-key, to the first communication message.

17. A system for secure communication between a first node and a second node with symmetric-key algorithm, wherein the second processing device is further configured to:

- encrypt a second communication message, with the symmetric-key, to the encrypted second communication message; and

- send the encrypted second communication message;

wherein the first processing device is further configured to:

- receive the encrypted second communication message;

- decrypt the encrypted second communication message, with the symmetric-key, to the second communication message.

18. A system according to either claim 16 or 17 wherein the first and second communication messages are transaction messages between the first node and second node for an online transaction between the first node and the second node.

19. Computer program comprising machine-readable instructions to cause a processing device to implement the method according to any one of claim 1 to 8.