

CLAIMS

1. A computer implemented method of encrypting data at an electronic device (S), the electronic device being associated with a key device (C), wherein the electronic device is further associated with a first asymmetric cryptography pair having a first electronic device private key (V_{1S}) and a first electronic device public key (P_{1S}), and the key device is associated with a second asymmetric cryptography pair having a first key device private key (V_{1C}) and a first key device public key (P_{1C}); the method comprising:
 - determining, at the electronic device, a deterministic key (DK);
 - receiving, at the electronic device, the first key device public key (P_{1C}) from the key device;
 - determining, at the electronic device, a second electronic device private key (V_{2S}) based on at least the first electronic device private key (V_{1S}) and the deterministic key (DK), and
 - determining, at the electronic device, a second key device public key (P_{2C}) based on at least the first key device public key (P_{1C}) and the deterministic key (DK);
 - determining a secret based on at least the second electronic device private key (V_{2S}) and the second key device public key (P_{2C});
 - encrypting the data at the electronic device using the determined secret or an encryption key that is based on the determined secret; and
 - sending information indicative of the deterministic key (DK) to the key device where the information can be stored.
2. The method of claim 1 further comprising: storing, at the key device, the information indicative of the deterministic key (DK).
3. The method of claim 1 or 2 wherein the deterministic key (DK) is based on a message (M).
4. The method of claim 3 comprising a step of generating the message (M) at the electronic device, and determining the deterministic key (DK) based on determining a hash of the message (M).

5. The method of any one of the preceding claims comprising a step of determining a second electronic device public key (P_{2S}) based on at least the first electronic device public key (P_{1S}) and the deterministic key (DK).
6. The method of any one of the preceding claims comprising: sending from the electronic device to the key device, a notice indicative of using a common elliptic curve cryptography (ECC) system with a common generator (G).
7. The method of claim 6 wherein the first electronic device public key (P_{1S}) and the first key device public key (P_{1C}) are based on elliptic curve point multiplication of the respective first electronic device private key (V_{1S}) and first key device private key (V_{1C}) and the common generator (G).
8. The method of claim 6 or 7 comprising a step of generating the first electronic device private key (V_{1S}) based on a random integer in an allowable range specified in the common ECC system; and generating the first electronic device public key (P_{1S}) based on elliptic curve point multiplication of the first electronic device private key (V_{1C}) and the common generator (G) according to the following formula:

$$P_{1S} = V_{1S} \times G$$

9. The method of any one of claims 6 to 8 comprising a step of generating the second electronic device private key (V_{2S}) based on a scalar addition of the first electronic device private key (V_{1S}) and the deterministic key (DK) according to the following formula:

$$V_{2S} = V_{1S} + DK$$

10. The method of any one of claims 6 to 9 comprising a step of generating the second electronic device public key (P_{2S}) based on at least the first electronic device public key (P_{1S}) with elliptic curve point addition to the deterministic key (DK).

11. The method of claim 10 wherein the second electronic device public key (P_{2S}) is based on the first electronic device 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:

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

12. The method of any one of claims 6 to 11 comprising a step of generating the second key device public key (P_{2C}) based on at least the first key device public key (P_{1C}) with elliptic curve point addition to the deterministic key (DK).
13. The method of claim 12 wherein the second key device public key (P_{2C}) is based on the first key device 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:

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

14. The method of any one of the preceding claims comprising a step of determining the encryption key based on the determined secret and identification information of the electronic device.
15. The method of any one of the preceding claims comprising a step of storing, at a data storage associated with the electronic device, the first key device public key (P_{1C}).
16. The method of any one of the preceding claims, the method further comprising:
 receiving, at the electronic device, the information indicative of the deterministic key (DK), from the key device;
 determining the secret based on the received information indicative of the deterministic key (DK); and
 decrypting, at the electronic device, the encrypted data using the secret or the

encryption key that is based on the secret.

17. The method of claim 16 comprising a step of generating, at the electronic device, an authentication message (M_A) and sending the authentication message (M_A) to the key device.
18. The method of claim 17 comprising a step of determining the deterministic authentication key (DK_A) by determining a hash of the message (M_A).
19. The method of any one of claims 16 to 18 comprising a step of generating, at the key device, a second asymmetric cryptography pair having a second key device private key (V_{2C}) and a second key device public key (P_{2C}).
20. The method of claim 18 and 19, wherein the second key device private key (V_{2C}) is based on the deterministic authentication key (DK_A) and the first key device private key (V_{1C}), and the second key device public key (P_{2C}) is based on the deterministic authentication key (DK_A) and the first key device public key (P_{1C}).
21. The method of claim 20 comprising:
 - generating, at the key device, a signed authentication message (SM_A) based on the deterministic authentication key (DK_A) and the second key device private key (V_{2C});
 - receiving, at the electronic device, the signed authentication message (SM_A) from the key device; and
 - validating the signed message (SM_A) with the second key device public key (P_{2C}); and authenticating the key device based on the result of validating the signed authentication message (SM_A).
22. The method of any one of claims 16 to 21 comprising:
 - requesting, at the electronic device, the information indicative of the deterministic key (DK) from the key device;
 - generating, at the key device, a signed message (SM) based on the message (M);

sending the signed message (SM) to the electronic device;
 validating, at the electronic device, the signed message (SM); and
 retrieving the message (M) such that the secret can be determined, at the electronic device, for decrypting the data.

23. A computer system for encrypting data at an electronic device, the computer system comprising:
 - the electronic device being associated with a first asymmetric cryptography pair having a first electronic device private key (V_{1S}) and a first electronic device public key (P_{1S}),
 - a key device being associated with a second asymmetric cryptography pair having a first key device private key (V_{1C}) and a first key device public key (P_{1C});
 - wherein the electronic device comprises a processor configured to:
 - o determine a deterministic key (DK);
 - o receive the first key device public key (P_{1C}) from the key device;
 - o determine a second electronic device private key (V_{2S}) based on at least the first electronic device private key (V_{1S}) and the deterministic key (DK), and
 - o determine a second key device public key (P_{2C}) based on at least the first key device public key (P_{1C}) and the deterministic key (DK);
 - o determine a secret based on at least the second electronic device private key (V_{2S}) and the second key device public key (P_{2C}); and
 - o encrypt the data on the electronic device using the determined secret or an encryption key that is based on the determined secret;
 - wherein information indicative of the deterministic key (DK) is stored on the key device.

24. The computer system of claim 23 further configured to decrypt data, the processor of the electronic device being configured to:
 - receive the information indicative of the deterministic key (DK), from the key device;
 - determine the secret based on the information indicative of the deterministic key (DK); and

decrypt the data using the determined secret or the encryption key that is based on the determined secret.

25. An electronic device for encrypting data, the electronic device being associated with a key device, wherein the electronic device is associated with a first asymmetric cryptography pair having a first electronic device private key (V_{1s}) and a first electronic device public key (P_{1s}), and the key device is associated with a second asymmetric cryptography pair having a first key device private key (V_{1c}) and a first key device public key (P_{1c}); the electronic device comprising a processing device configured to:
 - o determine a deterministic key (DK);
 - o receive the first key device public key (P_{1c}) from the associated key device;
 - o determine a second electronic device private key (V_{2s}) based on at least the first electronic device private key (V_{1s}) and the deterministic key (DK), and
 - o determine a second key device public key (P_{2c}) based on at least the first key device public key (P_{1c}) and the deterministic key (DK);
 - o determine a secret based on at least the second electronic device private key (V_{2s}) and the second key device public key (P_{2c}); and
 - o encrypt the data on the electronic device using the determined secret or an encryption key that is based on the determined secret;

- wherein information indicative of the deterministic key (DK) is sent to the key device where it can be stored.
26. A computer program comprising machine-readable instructions to cause a processing device of an electronic device to implement the method of any one of claims 1 to 22.