

## System and Method for Key Amplification

The invention relates to a system and method for key amplification and particularly, but not exclusively, for the amplification of quantum keys, where amplification refers to the process of using a key to generate a set of keys.

Keys are essential tools in the field of cryptography, used to encrypt and decrypt information sent from one party to another. Cryptographic keys often comprise a bit string and can be of different lengths. When a key is used for encryption, the strength of the encryption will depend on the security of the key. The security of a key can be contingent on a number of aspects of the key, for example, the generation of the key, the process of exchange of the key for encryption and decryption, the length of the key.

If a key is not to be easily guessed, the generation of the key needs to involve some random process, such as the use of a random number generator. The generation of the key should provide high entropy, or unpredictability, of the key.

The process of exchange of a key between entities should preferably be over a secured communication channel, which cannot be accessed by outside entities. However, many types of attack by outside entities exist and the security of a key during exchange cannot be guaranteed. This is particularly the case in quantum computing.

Methods for key exchange have, however, been developed that are not susceptible to an attack by a quantum computer. One such method is Quantum Key Distribution (QKD). However, QKD is dependent on an optical link and may suffer from low key exchange rates depending on the optical medium.

Ways in which to increase the security or entropy of cryptographic keys are constantly being sought.

According to a first aspect there is provided a method of key amplification by a first system and a second system of a network having a key to be amplified, a shared secret, a shared first system identity, a shared second system identity, a shared first key and a shared second key, comprising:

- (i) each system generating a new random number and creating a combination of the random number and the shared first key;
- (ii) each system using a shared predetermined process to generate a shared nonce derived from at least each system identity;
- (iii) each system using a shared predetermined process to generate a shared key and using the shared key to encrypt the combination with the shared nonce;
- (iv) each system receiving the encrypted combination from the other system;
- (v) each system using the shared key to decrypt the encrypted combination with the shared nonce to obtain the combination;
- (vi) each system generating a key of a set of keys which is a function of the combination of the first system, the combination of the second system, the shared second key and the shared secret, and
- (vii) each system repeating steps (i) to (vi) a predetermined number of times to generate further keys of the set of keys, which set of keys comprise an amplification of the key to be amplified.

The first system and the second system may share the secret by configuring each of the first and second systems with the shared secret. Configuring each of the first and second systems with a shared secret may comprise distributing the secret to the first and second systems in a secure environment.

The method may comprise each system encrypting the secret using an encryption algorithm and an identifier of the system as a key. The encryption algorithm may comprise a symmetric key encryption algorithm. The symmetric key encryption algorithm may be used in conjunction with one or more hash functions. The identifier of the system may be an immutable identifier of the system. The identifier of the system may comprise any of one or more physical characteristics of the system, one or more software signatures, a fingerprint of a physical unclonable function (PUF) of the system. The method may comprise each system storing the encrypted secret in a secure memory of the system.

The first system and the second system may share the first system identity and the second system identity by configuring each of the first and second systems with the first system identity and the second system identity. Configuring each of the first and second systems with the first system identity and the second system identity may comprise distributing the

first system identity and the second system identity to the first and second systems in a secure environment.

Each system may store the system identity of the other system in a secure memory.

For each system, the system identity may identify the system within the network. For each system, the system identity may comprise a characteristic of the system. The characteristic may be any of a physical characteristic of the system, a configurational characteristic of the system. The physical characteristic of the system may comprise a fingerprint of a PUF of the system. The configurational characteristic of the system may comprise one or more identifiers of one or more components of the system. The identifiers may comprise any of a MAC address of the system, a serial number identifier of a gateway of the system, a serial number identifier of a transceiver of the system.

For each system, the system identifier may comprise a challenge-response pair from a table of challenge-response pairs for a PUF of the other system. The tables may be stored in a secure memory. The first system may send a randomly chosen challenge to the PUF of the second system and verify a response of the second system against the table of challenge-response pairs. The second system may send a randomly chosen challenge to the PUF of the first system and verify a response of the first system against the table of challenge-response pairs.

The first system and the second system may connect to a key repository configured to hold one or more keys and retrieve the key to be amplified from the key repository. The key to be amplified may be a high entropy key. The key to be amplified may be generated using a quantum key distribution (QKD) process.

Each of the first and second systems may share the first key by using a predetermined algorithm to derive the first key from the key to be amplified. The first key may comprise a subset of the key to be amplified. The predetermined algorithm may comprise selecting a subset of the key to be amplified comprising selecting certain predetermined bits, for example, by applying a mask. The algorithm may further comprise an operation carried out on the predetermined bits comprising any of a predetermined permutation of the predetermined bits, a hash function of the predetermined bits, adding or multiplying the predetermined bits with a predetermined constant.

Each of the first and second systems may share the second key by using a predetermined algorithm to derive the second key from the key to be amplified. The second key may comprise a subset of the key to be amplified. The first key and the second key may be disjoint subsets of the key to be amplified. The predetermined algorithm may comprise selecting a subset of the key to be amplified comprising selecting certain predetermined bits, for example, by applying a mask. The algorithm may further comprise an operation carried out on the predetermined bits comprising any of a predetermined permutation of the predetermined bits, a hash function of the predetermined bits, adding or multiplying the predetermined bits with a predetermined constant. The predetermined bits, mask, operation carried out on the predetermined bits, the predetermined permutation, the hash function, the predetermined constant will be different from those used for the first key.

Each system generating a new random number may comprise the first system using a random number generator of the first system to generate a first system new random number and the second system using a random number generator of the second system to generate a second system new random number.

Each system creating a combination of the new random number and the shared first key may comprise creating a number which is a function of the new random number and the shared first key. The function may be a SHA-256 hash function. The function may be a derivation function comprising any of a hash derivation function, a block cipher derivation function. The function may be chosen to maximise the entropy of the combination of the random number and the shared first key.

Each system using the shared predetermined process to generate the shared nonce derived from each system identity may comprise combining each system identity with a value of a repetition marker which changes with each repetition. The value of the repetition marker may be a value of a counter or a value of a timestamp. In this way, in each repetition, each system generates a new nonce and the nonces are not reused. As the nonce of each system is generated using a changing value of the repetition marker, an element of freshness is introduced in each repetition of the steps. This helps prevent replay attacks on the first and second systems.

Each system using the shared predetermined process to generate the shared nonce derived from each system identity may comprise combining each system identity with a

value of a repetition marker which changes with each repetition and one or more parameters that are same for each system. Combining each system identity with a value of a repetition marker which changes with each repetition and one or more parameters that are same for each system may comprise concatenating each system identity with a value of a repetition marker which changes with each repetition and one or more parameters that are same for each system. The one or more parameters may comprise any of a network identity, a protocol name.

Each system using the shared predetermined process to generate the shared key may comprise using a key derivation function which is a function of the shared secret and the shared second key to generate the shared key. The key derivation function may comprise any of a HMAC-SHA256 function, a KMAC function, a CMAC function, a PBKDF2 function. The key derivation function is used on the shared second key, which is a subset of the key to be amplified which is different from the shared first key subset of the key to be amplified. This will help to prevent information leakage, since the shared first key is already employed in the function combining the random number and the shared first key.

Each system using the shared key to encrypt the combination with the shared nonce may comprise using a standard symmetric encryption algorithm. The standard symmetric algorithm may comprise AES-CCM.

Each system generating a key of a set of keys using the combination of the first system, the combination of the second system, the shared second key and the shared secret may comprise using a key derivation function to generate the key. The key derivation function may be any of hash based, password based. The key derivation function may comprise any of HKDF, scrypt, argon2, PBKDF.

In addition, a compression function may be applied to the key. The compression function may comprise any of a leftover hashing function, a Trevisan's extractor function, a strong blender function.

The use of the compression function will apply privacy amplification to the key.

Each system may repeat steps (i) to (vi) a predetermined number of times to generate a set of keys. The process of going from the key to the set of keys is amplification of the

key to be amplified.

In the steps of the method the shared system identities, the shared secret and the shared key are all used to exchange encrypted random numbers. Only with the knowledge of all three of these can the random numbers be correctly decrypted and then be used to create a set of keys shared between the systems. The aggregate length of the set of keys is increased by injecting the random numbers in a particular way that preserves, or improves, the randomness of the keys.

The key amplification method takes a relatively small key from a key repository and generates a set of keys with an aggregate length in excess of the length of the original key, thereby increasing an effective key exchange rate between the first and second systems, while preserving the entropy of the key. The method may generate a set of keys with high entropy.

According to a second aspect there is provided a first key amplification system and a second key amplification system of a network, having a key to be amplified, a shared secret, a shared first system identity, a shared second system identity, a shared first key and a shared second key, each system comprising:

- a random number generator configured to generate a random number;
- a combination engine configured to create a combination of the random number and the shared first key;
- a nonce generator configured to generate a shared nonce derived from at least each system identity;
- a key generator configured to generate a shared key;
- a cryptographic module configured to use the shared key to encrypt the combination with the shared nonce;
- a transceiver configured to send an encrypted combination to the other system and receive an encrypted combination from the other system;
- the cryptographic module configured to use the shared key to decrypt the encrypted combination with the shared nonce of the other system to obtain the combination, and
- the key generator configured to generate a key which is a function of the combination of the first system, the combination of the second system, the shared second key and the shared secret,

wherein the first and second systems repeatedly generate keys which form a set of keys which is an amplification of the key to be amplified.

The first and second key amplification systems may be configured with the shared secret. Configuring each of the first and second key amplification systems with the shared secret may comprise distributing the secret to the first and second systems in a secure environment.

The cryptographic module of each of the first and second key amplification systems may encrypt the secret using an encryption algorithm and an identifier of the system as a key. The encryption algorithm may comprise a symmetric key encryption algorithm. The symmetric key encryption algorithm may be used in conjunction with one or more hash functions. The identifier of the system may be an immutable identifier of the system. The identifier of the system may comprise any of one or more physical characteristics of the system, one or more software signatures, a fingerprint of a physical unclonable function (PUF) of the system. Each of the first and second key amplification systems may comprise a memory. The encrypted secret may be stored in the memory of each system.

The first and second key amplification systems may be configured with the first system identity and the second system identity. Configuring each of the first and second key amplification systems with the first system identity and the second system identity may comprise distributing the first system identity and the second system identity to the first and second systems in a secure environment. The system identities may be stored in the memory of each system.

For each key amplification system, the system identity may identify the system within the network. For each key amplification system, the system identity may comprise a physical characteristic of the system. The first and second key amplification systems may comprise a PUF. For each system, the physical characteristic of the system may comprise a fingerprint of a PUF of the system.

For each key amplification system, the system identity may comprise a configurational characteristic of the system. For each key amplification system, the configurational characteristic may comprise one or more identifiers of one or more components of the system. The identifiers may comprise any of a MAC address of the system, a serial

number identifier of a gateway of the system, a serial number identifier of a transceiver of the system.

For each key amplification system, the system identifier may comprise a challenge-response pair from a table of challenge-response pairs for a PUF of the other system. The tables may be stored in a secure memory. The first key amplification system may send a randomly chosen challenge to the PUF of the second key amplification system and verify a response of the second key amplification system against the table of challenge-response pairs. The second key amplification system may send a randomly chosen challenge to the PUF of the first key amplification system and verify a response of the first key amplification system against the table of challenge-response pairs.

The transceiver of each of the first and second key amplification systems may be configured to connect to a key repository configured to hold one or more keys and retrieve the key to be amplified from the key repository. The key to be amplified may be a high entropy key. The key to be amplified may be generated using a quantum key distribution (QKD) process.

The key generator of each of the first and second key amplification systems may be configured to use a pre-determined algorithm to derive the first key from the key to be amplified. The first key may comprise a subset of the key to be amplified. The predetermined algorithm may comprise selecting a subset of the key to be amplified comprising selecting certain predetermined bits, for example, by applying a mask. The algorithm may further comprise an operation carried out on the predetermined bits comprising any of a predetermined permutation of the predetermined bits, a hash function of the predetermined bits, adding or multiplying the predetermined bits with a predetermined constant.

The key generator of each of the first and second systems may be configured to use a pre-determined algorithm to derive the second key from the key to be amplified. The second key may comprise a subset of the key to be amplified. The first key and the second key may be disjoint subsets of the key to be amplified. The predetermined algorithm may comprise selecting a subset of the key to be amplified comprising selecting certain predetermined bits, for example, by applying a mask. The algorithm may further comprise an operation carried out on the predetermined bits comprising any of a

predetermined permutation of the predetermined bits, a hash function of the predetermined bits, adding or multiplying the predetermined bits with a predetermined constant. The predetermined bits, mask, operation carried out on the predetermined bits, the predetermined permutation, the hash function, the predetermined constant will be different from those used for the first key.

The combination engine of each of the first and second key amplification systems may be configured to create a combination of the random number and the shared first key by creating a number which is a function of the random number and the shared first key. The function may be a SHA-256 hash function. The function may be a derivation function comprising any of a hash derivation function, a block cipher derivation function. The function may be chosen to maximise the entropy of the blend of the random number and the shared first key.

The nonce generator of each of the first and second key amplification systems may be configured to use the shared predetermined process to generate the shared nonce derived from each system identity to combine each system identity with a value of a repetition marker which changes with each repetition. The value of the repetition marker may be a value of a counter or a value of a timestamp. In this way, in each repetition, each system generates a new nonce and the nonces are not reused. As the nonce of each system is generated using a changing value of the repetition marker, an element of freshness is introduced in each repetition of the steps. This helps prevent replay attacks on the first and second systems.

The nonce generator of each of the first and second key amplification systems may be configured to use the shared predetermined process to generate the shared nonce derived from each system identity to combine each system identity with a value of a repetition marker which changes with each repetition and one or more parameters that are same for each system. Combining each system identity with a value of a repetition marker which changes with each repetition and one or more parameters that are same for each system may comprise concatenating each system identity with a value of a repetition marker which changes with each repetition and one or more parameters that are same for each system. The one or more parameters may comprise any of a network identity, a protocol name.

The key generator of each of the first and second key amplification systems may be

configured to generate the shared key by using a key derivation function which is a function of the shared secret and the shared second key. The key derivation function may comprise any of a HMAC-SHA256 function, a KMAC function, a CMAC function, a PBKDF2 function.

The cryptographic module of each of the first and second key amplification systems may be configured to use the shared key to encrypt the combination with the shared nonce by using a standard symmetric encryption algorithm. The standard symmetric algorithm may comprise AES-CCM.

The key generator of each of the first and second key amplification systems may be configured to use a key derivation function to generate each key of the set of keys using the combination of the first system, the combination of the second system, the shared second key and the shared secret. The key derivation function may be any of hash based, password based. The key derivation function may comprise any of HKDF, scrypt, argon2, PBKDF.

The key generator of each of the first and second key amplification systems may be configured to apply a compression function to each key of the set of keys. The compression function may comprise any of a leftover hashing function, a Trevisan's extractor function, a strong blender function.

Embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is a schematic representation of a first key amplification system and a second key amplification system according to the second aspect, and

Figure 2 is a flow chart representation of the method of key amplification according to the first aspect.

Referring to Figure 1, a first key amplification system 1 comprises a random number generator 3, a combination engine 5, a nonce generator 7, a key generator 9, a cryptographic module 11, a transceiver 13, a memory 15 and a PUF 17. A second key amplification system 21 comprises a random number generator 23, a combination engine 25, a nonce generator 27, a key generator 29, a cryptographic module 31, a transceiver 33, a memory 35 and a PUF 37. The first and second key amplification systems 1, 21 are

part of a network. It will be appreciated that other key amplification systems may be comprised in the network. The key amplification systems may comprise devices of the network, such as gateway devices or any server connected to a network.

The first and second key amplification systems 1, 21 each have a key to be amplified, a shared secret, a shared first system identity, a shared second system identity, a shared first key and a shared second key.

The first and second key amplification systems 1, 21 are configured with the shared secret, by distribution of the secret to the systems in a secure environment.

The cryptographic module 11, 31 of each of the first and second key amplification systems 1, 21 encrypts the shared secret using an encryption algorithm and an identifier of the system as a key. In this embodiment, the identifier of each key amplification system 1, 21 comprises a fingerprint of the PUF 17, 37 of the system. The encrypted secret is stored in the memory 15, 35 of each system 1, 21.

The first and second key amplification systems 1, 21 are configured with the first system identity and the second system identity, by distribution of the first system identity and the second system identity to the systems in a secure environment. The system identities are stored in the memory 15, 35 of each key amplification system 1, 21. In this embodiment, the system identities comprise a fingerprint of the PUF 17, 37 of the system 1, 21.

The transceiver 13, 33 of each of the first and the second key amplification systems 1, 21 is configured to connect to a key repository (not shown) configured to hold one or more keys and retrieve the key to be amplified  $q$  from the key repository.

The key generator 9, 29 of each of the first and second key amplification systems 1, 21 is configured to use a pre-determined algorithm to derive the first key  $q'$  from the key  $q$ . The predetermined algorithm may comprise selecting a subset of the key to be amplified  $q$  comprising selecting certain predetermined bits, for example, by applying a mask. The algorithm may further comprise an operation carried out on the predetermined bits comprising any of a predetermined permutation of the predetermined bits, a hash function of the predetermined bits, adding or multiplying the predetermined bits with a predetermined constant.

The key generator 9, 29 of each of the first and second key amplification systems 1, 21 is configured to use a pre-determined algorithm to derive the second key  $q''$  from the key  $q$ . The first key  $q'$  and the second key  $q''$  each comprise a subset of the key to be amplified  $q$ . The predetermined algorithm may comprise selecting a subset of the key to be amplified  $q$  comprising selecting certain predetermined bits, for example, by applying a mask. The algorithm may further comprise an operation carried out on the predetermined bits comprising any of a predetermined permutation of the predetermined bits, a hash function of the predetermined bits, adding or multiplying the predetermined bits with a predetermined constant. The predetermined bits, mask, operation carried out on the predetermined bits, the predetermined permutation, the hash function, the predetermined constant will be different from those used for the first key.

Referring to Figure 2, the repetitions of the key amplification method carried out by the first and second key amplification systems 1, 21 to generate a set of keys is described.

In each repetition, each key amplification system 1, 21 generates a new random number. The random number generator 3, 23 of each system 1, 21 is configured to generate the new random number.

In each repetition, each key amplification system 1, 21 creates a combination of the random number and the shared first key  $q'$ . The combination engine 5, 25 of each system 1, 21 is configured to create the combination of the random number and the shared first key  $q'$ . This comprises, in this embodiment, creating a number which is a function of the random number and the shared first key  $q'$ . The function may be a SHA-256 hash function. The function may be a derivation function comprising any of a hash derivation function, a block cipher derivation function.

In each repetition, each key amplification system generates a shared nonce derived from the system identity. In this embodiment, the nonce generator 7, 27 of each system 1, 21 is configured to use a shared predetermined process to generate the shared nonce derived from each system identity to combine each system identity with a value of a repetition marker which changes with each repetition and one or more parameters that are same for each system. The value of the repetition marker may be a value of a counter or a value of a timestamp. In this way, in each repetition, each system generates a new nonce and the nonces are not reused. As the nonce of each system is generated using

a changing value of the repetition marker, an element of freshness is introduced in each repetition of the steps. This helps prevent replay attacks on the first and second systems. Combining each system identity with a value of a repetition marker which changes with each repetition and one or more parameters that are same for each system may comprise concatenating each system identity with a value of a repetition marker which changes with each repetition and one or more parameters that are same for each system. The one or more parameters may comprise any of a network identity, a protocol name.

In each repetition, each key amplification system 1, 21 generates a shared key. The key generator 9, 29 of each system 1, 21 is configured to generate the shared key. Each shared key is generated by using a shared predetermined process comprising using a key derivation function K which is a function of the shared secret and the shared second key to generate the shared key. The key derivation function K may comprise any of a HMAC-SHA256 function, a KMAC function, a CMAC function, a PBKDF2 function.

In each repetition, each key amplification system 1, 21 uses the shared key to encrypt the combination with the shared nonce. The cryptographic module 11, 31 of each system 1, 21 is configured to use the shared key to encrypt the combination with the shared nonce. A standard symmetric encryption algorithm, such as AES-CCM is used.

In each repetition, each key amplification system 1, 21 receives the encrypted combination from the other system. The transceiver 13, 33 of each system 1, 21 is configured to send an encrypted combination to the other system and receive an encrypted combination from the other system.

In each repetition, the cryptographic module 11, 31 of each key amplification system 1, 21 uses the shared key to decrypt the encrypted combination with the shared nonce to obtain the combination.

In each repetition, each key amplification system 1, 21 generates a key which is a function of the combination of the first system, the combination of the second system, the shared second key  $q''$  and the shared secret. The key generator 9, 19 of each system 1, 21 is configured to generate the key using a key derivation function. The key derivation function may be any of hash based, password based. The key derivation function may comprise any of HKDF, scrypt, argon2, PBKDF.

In each repetition, in addition, a compression function may be applied to the key. The compression function may comprise any of a leftover hashing function, a Trevisan's extractor function, a strong blender function. The use of the compression function will apply privacy amplification to the key.

Each key amplification system 1, 21 repeating the steps a predetermined number of times generates a set of keys which comprise an amplification of the key to be amplified,  $q$ . This produces a set of keys from the key to be amplified  $q$  thereby amplifying the key  $q$ .

## CLAIMS

1. A method of key amplification by a first system and a second system of a network having a key to be amplified, a shared secret, a shared first system identity, a shared second system identity, a shared first key and a shared second key, comprising:
  - (i) each system generating a new random number and creating a combination of the new random number and the shared first key;
  - (ii) each system using a shared predetermined process to generate a shared nonce derived from at least each system identity;
  - (iii) each system using a shared predetermined process to generate a shared key and using the shared key to encrypt the combination with the shared nonce;
  - (iv) each system receiving the encrypted combination from the other system;
  - (v) each system using the shared key to decrypt the encrypted combination with the shared nonce to obtain the combination;
  - (vi) each system generating a key of a set of keys which is a function of the combination of the first system, the combination of the second system, the shared second key and the shared secret, and
  - (vii) each system repeating steps (i) to (vi) a predetermined number of times to generate further keys of the set of keys which set of keys comprise an amplification of the key to be amplified.
2. A method according to claim 1 in which the first system and the second system share the secret by configuring each of the first and second systems with the shared secret in a secure environment.
3. A method according to claim 1 or claim 2 comprising each system encrypting the secret using an encryption algorithm and an identifier of the system as a key, wherein the identifier of the system comprises any of one or more physical characteristics of the system, one or more software signatures, a fingerprint of a physical unclonable function (PUF) of the system.
4. A method according to any preceding claim in which the first system and the second system share the first system identity and the second system identity by configuring each of the first and second systems with the first system identity and the second system identity in a secure environment.

5. A method according to any preceding claim in which the first system and the second system connect to a key repository configured to hold one or more keys and retrieve the key to be amplified from the key repository.
6. A method according to any preceding claim in which each of the first and second systems share the first key by using a pre-determined algorithm to derive the first key from the key to be amplified and share the second key by using a pre-determined algorithm to derive the second key from the key to be amplified.
7. A method according to any preceding claim in which the shared first key is a subset of the key to be amplified and the shared second key is a subset of the key to be amplified.
8. A method according to any preceding claim in which each system creating a combination of the new random number and the shared first key comprises creating a number which is a function of the random number and the shared first key.
9. A method according to any preceding claim in which each system generates the shared nonce derived from at least each system identity using a shared predetermined process by combining each system identity with a value of a repetition marker which changes with each repetition.
10. A method according to claim 9 in which each system generates the shared nonce derived from at least each system identity using the shared predetermined process by combining each system identity with the value of the repetition marker which changes with each repetition and one or more parameters that are same for each system.
11. A method according to any preceding claim in which, in each repetition, each system uses the shared predetermined process to generate the shared nonce derived from at least each system identity and a value of a repetition marker which changes with each repetition.
12. A method according to any preceding claim in which each system uses the shared predetermined process to generate the shared key by using a key derivation function which is a function of the shared secret and the shared second key.

13. A method according to any preceding claim in which each system generating a key of the set of keys using the combination of the first system, the combination of the second system, the shared second key and the shared secret comprises using a key derivation function to generate the key.

14. A method according to claim 13 in which a compression function is applied to the key of the set of keys.

15. A first key amplification system and a second key amplification system of a network, having a key to be amplified, a shared secret, a shared first system identity, a shared second system identity, a shared first key and a shared second key, each system comprising:

- a random number generator configured to generate a random number;

- a combination engine configured to create a combination of the random number and the shared first key;

- a nonce generator configured to generate a shared nonce derived from at least each system identity;

- a key generator configured to generate a shared key;

- a cryptographic module configured to use the shared key to encrypt the combination with the shared nonce;

- a transceiver configured to send an encrypted combination to the other system and receive an encrypted combination from the other system;

- the cryptographic module configured to use the shared key to decrypt the encrypted combination with the shared nonce of the other system to obtain the combination, and

- the key generator configured to generate a key which is a function of the combination of the first system, the combination of the second system, the shared second key and the shared secret,

wherein the first and second systems repeatedly generate keys which form a set of keys which is an amplification of the key to be amplified.